



3Com® X Family Local Security Manager User's Guide



X5 (25-user license) – 3CRTPX5-25-96
X5 (unlimited license) – 3CRTPX5-U-96
X506 – 3CRX506-96

Version 2.5.1

Part Number TECHD-176 Rev B01
Published April 2007

<http://www.3com.com/>



3Com Corporation
350 Campus Drive
Marlborough, MA 01752-
3064

Copyright © 2005–2007, 3Com Corporation and its subsidiaries. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms, or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hardcopy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGENDS:

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

United States Government Legend: All technical data and computer software is commercial in nature and developed solely at private expense. Software is delivered as Commercial Computer Software as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, the 3Com logo, TippingPoint, the TippingPoint logo, and Digital Vaccine are registered trademarks of 3Com Corporation or one of its subsidiaries.

Microsoft and Windows are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Oracle is a registered trademark of Oracle Corporation.

Other brand and product names may be registered trademarks or trademarks of their respective holders.

Contents

About This Guide	xi
Target Audience	xi
Knowledge, Skills, and Abilities	xi
Conventions	xii
Cross References	xii
Internal Cross References	xii
External Cross References	xii
Typeface	xii
Procedures	xii
Menu Navigation	xiii
Sample Procedure	xiii
Screen Captures	xiii
Messages	xiii
Warning	xiii
Caution	xiii
Note	xiv
Tip	xiv
Related Documentation	xiv
Online Help	xiv
Customer Support	xiv
Contact Information	xv
 Chapter 1. System Overview	 1
Overview	1
X Family Device	1
Core Functionality	2
X Family Environment	3
Local Clients	4
System Requirements	4
SMS Configuration	4
 Chapter 2. LSM Navigation	 5
Overview	5
Security Notes	5
Logging In	6
LSM Screen Layout	8
Main Menu Bar	9
Navigation	10
Content and Functionality	11
Title Bar	11

Tabbed Menu Options	11
System Summary	12
System Status	12
Health	12
Packet Stats	13
Network DHCP	13
Reboot Device	13
Log Summary	13
Product Specifications	14

Chapter 3. IPS Filtering **15**

Overview	15
Using the IPS	16
Security Profiles	17
Managing Security Profiles	19
Security Profile Details	20
IPS Digital Vaccine (DV) Filters	23
Configuring DV Filters	25
View DV Filters	26
Filter Search	27
Filters List (All Filters)	27
View Filter Overrides and Custom Settings	29
Edit DV Filter Category Settings	29
Configure Filter Limits/Exceptions based on IP Address	34
Reset an Individual Filter	35
Port Scan/Host Sweep Filters	35
Traffic Threshold Filters	38
Managing Traffic Threshold Filters	39
Create or Edit a Traffic Threshold Filter	41
Action Sets	44
Managing Actions	47
Rate Limit Action Set	49
Quarantine Action Set	49
Notification Contacts	52
Alert Aggregation and the Aggregation Period	52
IPS Services	55
Preferences	57
Reset Filters	57
Configure Threat Suppression Engine (TSE)	58
Adaptive Filter Configuration	60
How Adaptive Filtering Works	60

Chapter 4. Firewall **63**

Overview	63
How Firewall Rule Enforcement Works	64
Default Firewall Rules	67

Managing Firewall Rules	68
Configuring Firewall Rules	71
Firewall Services	75
Firewall Services Page Field Descriptions	77
Configuring Service Groups	78
Schedules	79
Firewall Schedules Page Field Descriptions	80
Managing Schedules	81
Virtual Servers	82
Virtual Servers page	83
Virtual Servers Summary Information	83
Configuring Virtual Servers	84
Web Filtering	85
How Web Filtering Works	86
Setting Up Web Filtering	87
Web Filtering Page	88
Web Filtering General Configuration Parameters	89
Web Filter Service	90
Custom Filter List	92
Custom Filter List Configuration Parameters and Functions	93
Configure URL Patterns	94
URL Test	96

Chapter 5. Events: Logs, Traffic Streams, Reports 97

Overview	98
Logs	98
Alert Log	99
Audit Log	100
IPS Block Log	101
Firewall Block Log	102
Firewall Session Log	103
VPN Log	104
Configuration	104
System Log	105
Configuring Remote System Logs	105
Managing Logs	106
Viewing Logs	107
Downloading a Log	107
Resetting a log	108
Searching a Log	109
Managed Streams	110
Blocked Streams	110
Rate Limited Streams	112
Quarantined Addresses	113
Health	116
Device Health	117

Memory and Disk Usage	117
Module Health	118
Performance/Throughput	120
Port Health	120
Reports	121
Attack Reports	122
Rate Limit Reports	123
Traffic Reports	123
Traffic Threshold Report	125
Quarantine Report	125
Configure Adaptive Filter Events Report	125
Firewall Reports	126

Chapter 6. Network 129

Overview	129
Configuration Overview	130
Deployment Modes	131
Network Port Configuration	132
Port Configuration Tasks	133
Troubleshoot Port Link-Down errors	134
Security Zone Configuration	135
Creating, Editing and Configuring Security Zones	136
IP Interfaces	140
Configuration Overview	140
Managing IP Interfaces	141
IP Addresses: Configuration Overview	142
Internal Interface: Static IP Address	143
External Interface: Static IP Address Configuration	144
External Interface: DHCP Configuration	145
External Interface: PPTP Client Configuration	145
External Interface: L2TP Client Configuration	146
External Interface: PPPoE Client Configuration	147
Configuring a GRE Tunnel	148
Manage Security Zones for IP Interfaces	149
Configuring Routing for IP Interfaces	150
Bridge Mode for IP Interfaces	150
RIP for IP Interfaces	150
Multicast Routing for IP Interfaces	152
IP Address Groups	153
DNS	155
Default Gateway	156
Routing	157
Overview	157
Routing Table	157
Static Routes	159
RIP Setup	160

Multicast (IGMP and PIM-DM)	163
IGMP Setup	163
PIM-DM Setup	165
Default Gateway	167
DHCP Server	167
Overview	167
DHCP Server Page	168
Configure DHCP Server	169
DHCP Relay	171
Configuring DHCP Relay	172
Static Reservations	174
Network Tools	176
DNS Lookup	177
Find Network Path	177
Traffic Capture	177
Ping	178
Traceroute	179

Chapter 7. VPN **181**

Overview	181
About VPN	182
VPN Connection Security Features	182
VPN Configuration Overview	183
IPSec Configuration	184
IPSec Status Details	185
IPSec Configuration	187
Configure an IPSec Security Association	189
IKE Proposal	198
Manage IKE Proposals	198
Configuring IKE Proposals	200
L2TP Configuration	208
Overview	208
L2TP Status	208
L2TP Server Configuration	210
PPTP Configuration	212
Overview	212
PPTP Status	212
PPTP Server Configuration	213

Chapter 8. System **217**

Overview	217
Update TOS and Digital Vaccine Software	218
Viewing and Managing Current TOS and DV Software	219
Rolling Back to a Previous TOS Version	220
Download and Install a TOS or Digital Vaccine Update	221
Updating the Digital Vaccine (Filters)	222

Updating the TOS Software	224
System Snapshots	227
Time Options	229
Internal CMOS Clock	231
NTP Server	231
Time Zones	232
SMS/NMS	232
High Availability	235
How High Availability Works	236
Failover Operation	236
Standby Operation	236
Polling	237
Configuration Overview	237
Configuring High Availability with AutoDV	239
Troubleshooting High Availability with AutoDV	239
Thresholds to Monitor Memory and Disk Usage	239
Email Server	241
Syslog Servers	242
Setup Wizard	242

Chapter 9. Authentication 245

Overview	246
User List	246
Overview	246
TOS and Local User Accounts	247
TOS User Security Level	247
Username and Password Requirements	248
Managing User Accounts	249
How Local User Authentication Works:	
RADIUS, Privilege Groups and X.509 Certificates	251
Overview	251
RADIUS	252
Privilege Groups	253
X.509 Certificates	255
Overview	255
Configuring X.509 Certificates	256
CA Certificates	257
Certificate Revocation List (CRL) for a CA Certificate	258
Certificate Requests	260
Managing Certificate Requests	262
Local Certificates	263
Preferences	266

Appendix A. Browser Certificates 271

Overview	271
Client Authentication Message	272

Security Alert	273
Certificate Authority	274
Invalid Certificate Name	277
Example - Creating Personal Certificate	279
Appendix B. Web Filter Service	281
Overview	281
Core Categories	282
Productivity Categories	284
Available Productivity Categories	284
Purchasing a Web Filter License	289
Appendix C. Log Formats and System Messages	291
Overview	291
Log Formats	292
Alert and IPS Block Log Formats	292
Audit Log Format	294
Firewall Block Log Format	296
Firewall Session Log Format	298
VPN Log Format	299
System Log Format	300
Remote Syslog Log Format	301
High Availability Log Messages	302
System Update Status Messages	303
Appendix D. Device Maximum Values	305
Glossary	307
Index	315

About This Guide

Explains who this guide is intended for, how the information is organized, where information updates can be found, and how to obtain customer support if you cannot resolve a problem.

Welcome to the Local Security Manager (LSM). The LSM is the control center from which you can configure, monitor, and report on the X family devices in your network.

This section covers the following topics:

- [“Target Audience” on page xi](#)
- [“Conventions” on page xii](#)
- [“Related Documentation” on page xiv](#)
- [“Customer Support” on page xiv](#)

Target Audience

This guide is intended for administrators who manage one or more X family devices.

Knowledge, Skills, and Abilities

This guide assumes you, the reader, are familiar with general networking concepts and the following standards and protocols:

- TCP/IP
- UDP
- ICMP
- Ethernet
- Simple Network Time Protocol (SNTP)
- Simple Mail Transport Protocol (SMTP)
- Simple Network Management Protocol (SNMP)

Conventions

This guide follows several procedural and typographical conventions to better provide clear and understandable instructions and descriptions. These conventions are described in the following sections.

This book uses the following conventions for structuring information:

- [Cross References](#)
- [Typeface](#)
- [Procedures](#)
- [Messages](#)

Cross References

When a topic is covered in depth elsewhere in this guide, or in another guide in this series, a cross reference to the additional information is provided. Cross references help you find related topics and information quickly.

Internal Cross References

This guide is designed to be used as an electronic document. It contains cross references to other sections of the document that act as hyperlinks when you view the document online. The following text is a hyperlink: [Procedures](#).

External Cross References

Cross references to other publications are not hyperlinked. These cross references will take the form: see <chapter name > in the *Publication Name*.

Typeface

This guide uses the following typeface conventions:

Bold	used for the names of screen elements like buttons, drop-down lists, or fields. For example, when you are done with a dialog, you would click the OK button. See Procedures below for an example.
<code>Code</code>	used for text a user must type to use the product
<i>Italic</i>	used for guide titles, variables, and important terms
Hyperlink	used for cross references in a document or links to web site

Procedures

This guide contains several step-by-step procedures that tell you how to perform a specific task. These procedures always begin with a phrase that describes the task goal, followed by numbered steps that describe what you must do to complete the task.

The beginning of every chapter has cross references to the procedures that it contains. These cross references, like all cross references in this guide, are hyperlinked.

Menu Navigation

The LSM provides drop-down menu lists to navigate and choose items in the user interface. Each instruction that requires moving through the menus uses an arrow (>) to indicate the movement. For example, **Edit > Details** means, select the **Edit** menu item. Then, click the **Details** option.

Sample Procedure

STEP 1 Click the **Filters** tab.

STEP 2 Place your mouse cursor over the **Open** menu.

Screen Captures

The instructions and descriptions in this document include images of screens. These screen captures may be cropped, focusing on specific sections of the application, such as a pane, list, or tab. Refer to the application for full displays of the application.

Messages

Messages are special text that are emphasized by font, format, and icons. There are four types of messages in this guide:

- [Warning](#)
- [Caution](#)
- [Note](#)
- [Tip](#)

A description of each message type with an example message follows.

Warning

Warnings tell you how to avoid physical injury to people or equipment. For example:



WARNING The push-button on/off power switch on the front panel of the server does not turn off the AC power. To remove AC power from the server, you must unplug the AC power cord from either the power supply or the wall outlet.

Caution

Cautions tell you how to avoid a serious loss of data, time, or security. You should carefully consider this information when determining a course of action or procedure. For example:



CAUTION You should disable password caching in the browser you use to access the LSM. If you do not disable password caching in your browser, and your workstation is not secured, your system security may be compromised.

Note

Notes tell you about information that might not be obvious or that does not relate directly to the current topic, but that may affect relevant behavior. For example:



Note If the device is not currently under SMS control, you can find out the IP address of the last SMS that was in control by checking SMS & NMS page (**System > Configuration > SMS/NMS**).

Tip

Tips are suggestions about how you can perform a task more easily or more efficiently. For example:



TIP You can see what percentage of disk space you are using by checking the Monitor page (**Events > Health > Monitor**).

Related Documentation

The X family products have a full set of documentation. These publications are available in electronic format on your CD. For the most recent updates, check the Threat Management Center (TMC) web site at <https://tmc.tippingpoint.com>.

Online Help

In the Launch Bar of the application, the Help button opens the main welcome page to the online help.



Opens the online help at the opening page.

If you have problems finding help on a particular subject, you can review the Index or use the Search tab in the navigation pane. Each page also includes related topic links to find more information on particular subjects and functions.

Customer Support

We are committed to providing quality customer support to all customers. A customer is provided with detailed customer and support contact information. For the most efficient resolution of your problem,

please take a moment to gather some basic information from your records and from your system before contacting customer support.

Information	Location
Your X family device serial number	You can find this number in the LSM in the <i>System Summary</i> page, on the shipping invoice that came with the device, or on the bottom of the device.
Your TOS version number	You can find this information in the LSM in the Device Summary page, or by using the CLI <code>show version</code> command.
Your X family device boot time	You can find this information in the LSM in the System Summary page.

Contact Information

Please address all questions regarding the software to your authorized representative.

1 System Overview

The X family device is a high-speed, comprehensive security system with a browser-based manager called the Local Security Manager (LSM). The Overview section provides an overview of the LSM functions and use in the X family device.

Overview

Enterprise security schemes once consisted of a conglomeration of disparate, static devices from multiple vendors. Today, the X family device provides the advantages of a single, integrated, highly adaptive security system that includes powerful hardware and an intuitive management interface.

This section describes the X family device and the LSM client application, Command Line Interface (CLI), and Security Management System (SMS) used to interact with and manage the device.

The Overview chapter includes the following topics:

- [“X Family Device” on page 1](#)
 - [“Core Functionality” on page 2](#)
 - [“X Family Environment” on page 3](#)
 - [“Local Clients” on page 4](#)
- [“System Requirements” on page 4](#)
- [“SMS Configuration” on page 4](#)



Note Check the Release Notes for specific limitations and known issues regarding the current release.

X Family Device

The X family device offers an integrated system that includes a stateful packet inspection firewall, IPSec virtual private network (VPN) management, bandwidth management, and web content filtering functions along with TippingPoint Intrusion Prevention System (IPS) functionality.

The X family firewall functionality provides service-level, stateful inspection of network traffic. It incorporates filtering functionality to protect mission-critical applications. An administrator can use firewalls and content filters to determine how the device handles traffic to and from a particular service. These filters are specified by the source, destination, and service or protocol of the traffic. The device maintains an inventory of the active hosts and services on those hosts.

IPSec VPN management provides the ability to apply all X family functionality across the enterprise, monitoring network traffic at the enterprise level and also traffic between main office and branch locations.

Bandwidth management, or policy-based traffic shaping, allows the X family device to control both inbound and outbound traffic streams as well as inside and outside IPSec VPN tunnels. Using these policies, the device allows users to prioritize real-time business critical applications including video and conferencing, IP telephony, and interactive distance-learning over non-essential traffic, such as peer-to-peer file sharing.

Web content filtering provides the tools to enforce network policy by prohibiting the download of non-work related web sites and offensive or illegal web content.

The IPS functionality provides total packet inspection and intrusion prevention to detect and block malicious traffic such as worms, viruses, Trojans, Phishing attempts, Spyware, and VoIP threats. Using filters defined by the Digital Vaccine security team, the X family device scans traffic to recognize header or data content that signals an attack along with the protocol, service, and the operating system or software the attack affects. Each filter includes an action set, which determines how the device responds when it detects packets that match filter parameters. In a broad sense, the device either drops matching packets or permits them. The Digital Vaccine security team continually develops new attack filters to preemptively protect against the exploit of new and zero day vulnerabilities. To ensure up-to-date network protection, you can configure the device to automatically check for and install DV updates.

Core Functionality

The X family device provides the following core functionality:

- Stateful packet inspection firewall — flexible configuration of object-based firewall rules and unified control of multiple services, virtual servers, network address translation (NAT), and routing.
- Security Zones — logically section your network for the purposes of applying firewall rules and IPS filters between internal sections of your network, between your network and the internet, and between your network and remote office locations (VPN).
- Standards-based IPSec Virtual Private Networks including:
 - hardware-accelerated encryption DES, 3DES, and AES encryption protocols
 - feature-rich client VPN capability using PPTP or L2TP protocols
 - ability to inspect and control traffic both inside and outside of all VPN tunnel types using firewalls or IPS to ensure secure VPN connectivity.
- Flexible user authentication — control access to the device and the internet, authenticating via the device itself, or through an external RADIUS database.
- Web filtering — URL filtering with configurable permit/block lists and regular-expression URL matching as well as a web content filtering subscription service to enforce network security and

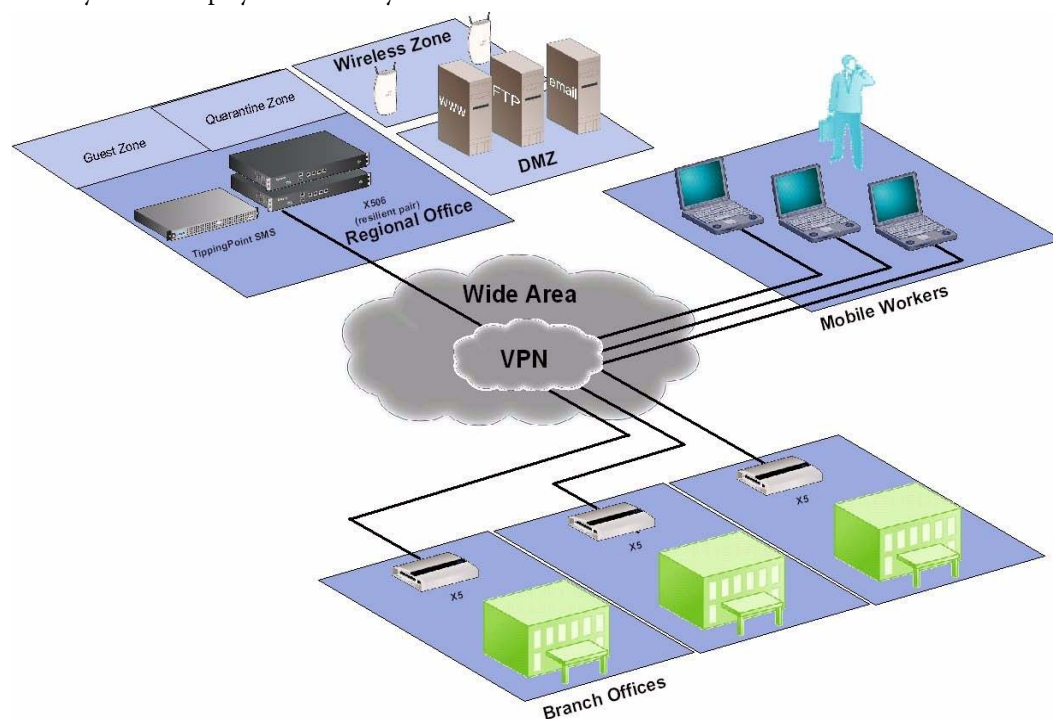
usage policy by prohibiting the download of non-work related web sites and offensive or illegal Web content.

- Bandwidth management — enforce network usage policy by rate-limiting applications such as peer-to-peer file sharing and instant messaging applications.
- Prioritization of traffic inside and outside VPN tunnels with flexible, policy-based controls.
- IP multicast routing (PIM-DIM) over IPsec, supporting next-generation IP conferencing applications — prioritizes real-time traffic and provides secure connectivity for IP multicast traffic.
- Device management — option to configure, monitor, and manage the device using either the web-based client application (the Local Security Manager) or the command line interface (CLI).
- Centralized Management — option to configure, monitor, and manage individual or multiple X family devices using the Security Management System (SMS).
- The TippingPoint Intrusion Prevention System (IPS) — identify and stop malicious traffic on the edge of the network using filters that detect and block malicious traffic. Customize default filters to meet the specific needs of your enterprise.
- Digital Vaccine real-time protection — the Threat Management Center monitors global network security threats and continually develops new attack filters which are automatically distributed to preemptively protect against the exploit of new and zero day vulnerabilities.

The following sections describe the X family environment and system components in more detail.

X Family Environment

An X family device can be installed at the perimeter of your network, in your remote offices, on your intranet, or in all three locations. The following diagram shows an example of a corporate network with X family devices deployed in a variety of locations.



When the X family device is installed and configured, it protects your network zones (LAN, WAN, and VPN, for example) using firewall rules and IPS filters. The device scans and reacts to network traffic according to the actions configured in the firewall rule or IPS filter. Each security zone and device can use a different set of firewall rules and IPS filters. Actions configured on the firewall rules and IPS filters provide the instructions for the device and can include blocking, rate limiting, or permitting the traffic and sending a notification about the action to a device or e-mail address. Options are also available to block traffic and quarantine the source IP address for the traffic.

For users who will deploy multiple X family devices across the enterprise, TippingPoint provides the Security Management System (SMS). The SMS allows you to coordinate the management of multiple devices for administration, configuration, and monitoring. Most importantly, the SMS includes enterprise-wide reporting and trend analysis.

Local Clients

You can access the X family device for monitoring, management, and configuration from any of the following three client applications:

- **Local Security Manager (LSM)** — Web-based GUI for managing one IPS device. The LSM provides HTTP and HTTPS (secure management) access. This access requires Microsoft Internet Explorer 6.0 or later, Firefox 1.5+, Mozilla 1.7+, or Netscape 8.1+. Using the LSM, you have a graphical display for reviewing, searching, and modifying settings. The GUI interface also provides graphical reports for monitoring the device traffic, triggered filters, and packet statistics.
- **Command Line Interface (CLI)** — Command line interface for reviewing and modifying settings on the device. The CLI is accessible through Telnet and SSH (secure access).
- **Secure Management System (SMS)** — the SMS allows you to remotely manage multiple X family devices. You can configure security zones, profiles and policy (firewall rules and IPS filters) from the SMS and distribute the configuration to multiple devices. The SMS also allows you to view, manage and edit device configuration, and review logs and reports for all devices under SMS management.



Note The device allows for 10 web client connections, 10 telnet/SSH (for CLI) connections, and one console connection at once.

System Requirements

The LSM is software accessed using a web browser. The browser's hardware and software requirements are not as technical as systems loading the software locally. To access the LSM, you need the following:

- Microsoft Internet Explorer (MSIE) v 6.0 or greater with 128-bit encryption and support for JavaScript and cookies, Firefox 1.5+, Mozilla 1.7+, or Netscape 8.1+

SMS Configuration

If you will maintain your device using the Security Management System (SMS) or you will no longer use the SMS, you need to configure a setting on the device. This setting identifies if the device is controlled by the SMS.

For more information, see [“SMS/NMS” on page 232](#).

2 LSM Navigation

LSM Navigation describes the LSM interface, how to log in, and the general sections of the application.

Overview

The Local Security Manager (LSM) is a graphical user interface (GUI) that makes configuring and monitoring your X family device easy by providing a user-friendly interface to help accomplish administrative activities. You access the LSM through a browser. See [“Log in to the LSM” on page 6](#) for more information.

This chapter details the login and navigation procedures of the LSM user interface. It includes the following information:

- [“Security Notes” on page 5](#)
- [“Logging In” on page 6](#)
- [“LSM Screen Layout” on page 8](#)
- [“System Summary” on page 12](#)

Security Notes

The LSM enables you to manage your X family device using a Web browser. It is important to note that some browser features, such as password caching, are inappropriate for security use and should be turned off.



CAUTION Some browsers offer a feature that stores your user login and password for future use. We recommend that you turn this feature off in your browser. It is counter to standard security practices to store login names and passwords, especially those for sensitive network equipment, on or near a workstation.

In addition, you can configure the LSM to communicate using either an HTTP or an HTTPS server. The default configuration is to use an HTTPS server. Whenever the device is connected to your network, you should run the HTTPS server, not the HTTP server. HTTP servers are not secure because your user name and password travel over your network unencrypted. You should only use the HTTP server when you are sure that communications between the device and the workstation from which you access the LSM cannot be intercepted.



Note You can modify the server configuration using the **conf t server** command. For details, see the **Command Line Interface Reference Guide**.

Logging In

When you log in to the LSM, you are prompted for your username and your password. This login gives you access to the areas of the LSM permitted by your user role. For information on user roles and accesses, see [Chapter 9, “Authentication”](#).



TIP Most Web browsers will not treat addresses beginning with HTTP and HTTPS interchangeably. If your browser cannot find your LSM, make sure that you are using `http://` or `https://` depending on which Web server you are running.



Note The device supports up to 10 Web client connections, 10 telnet/SSH (for CLI) connections, and 1 console connection at once.

Depending on your security settings, warnings may display when accessing the client. To access the device without warnings, refer to [Appendix A, “Browser Certificates”](#).

You will be presented with the login screen under the following situations:

- When you first log in to the LSM
- After the LSM web session times out

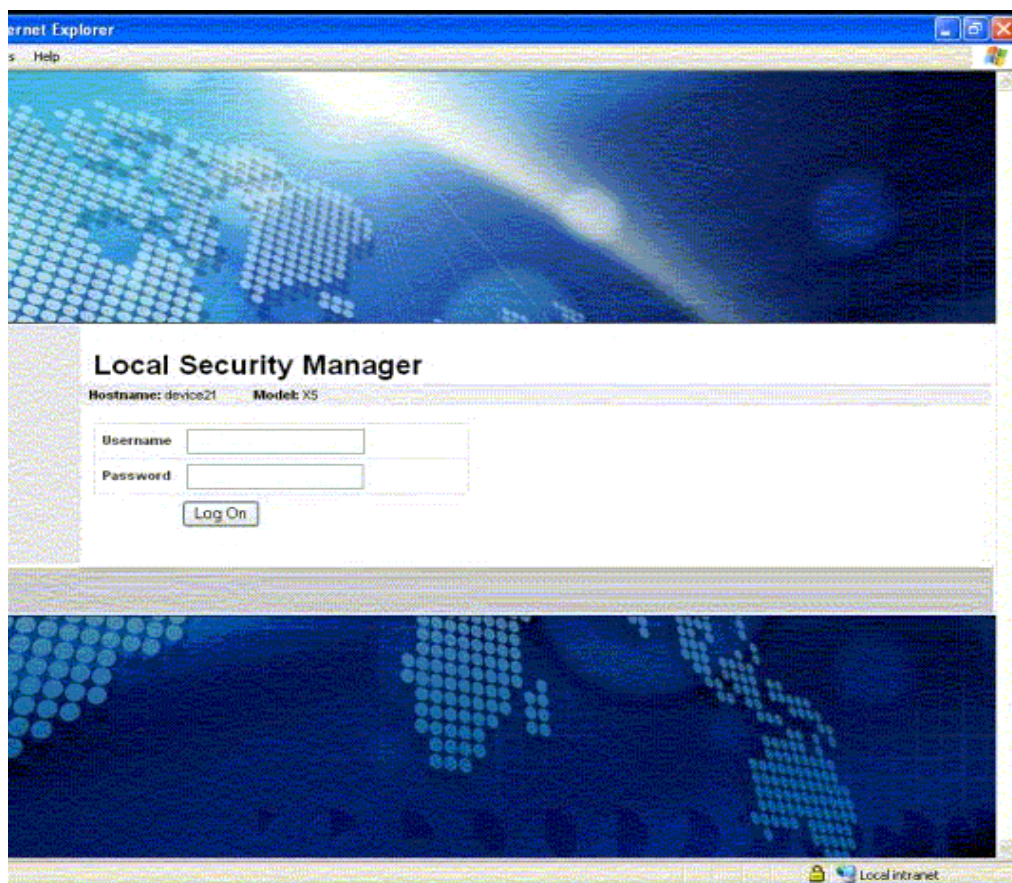
Log in to the LSM

STEP 1 Enter the IP address or hostname of your IPS device in your browser **Address** bar. For example:

```
https://123.45.67.89
```

The LSM displays a login page. The page provides the name and model of your device.

Figure 2–1: LSM Logon Page



STEP 2 Enter your **Username**.

STEP 3 Enter your **Password**

STEP 4 Click **Log On**.

The LSM validates your account information against the permitted users of the software. If the information is valid, the LSM software opens. If the account information is not valid, the Login page is redisplayed.



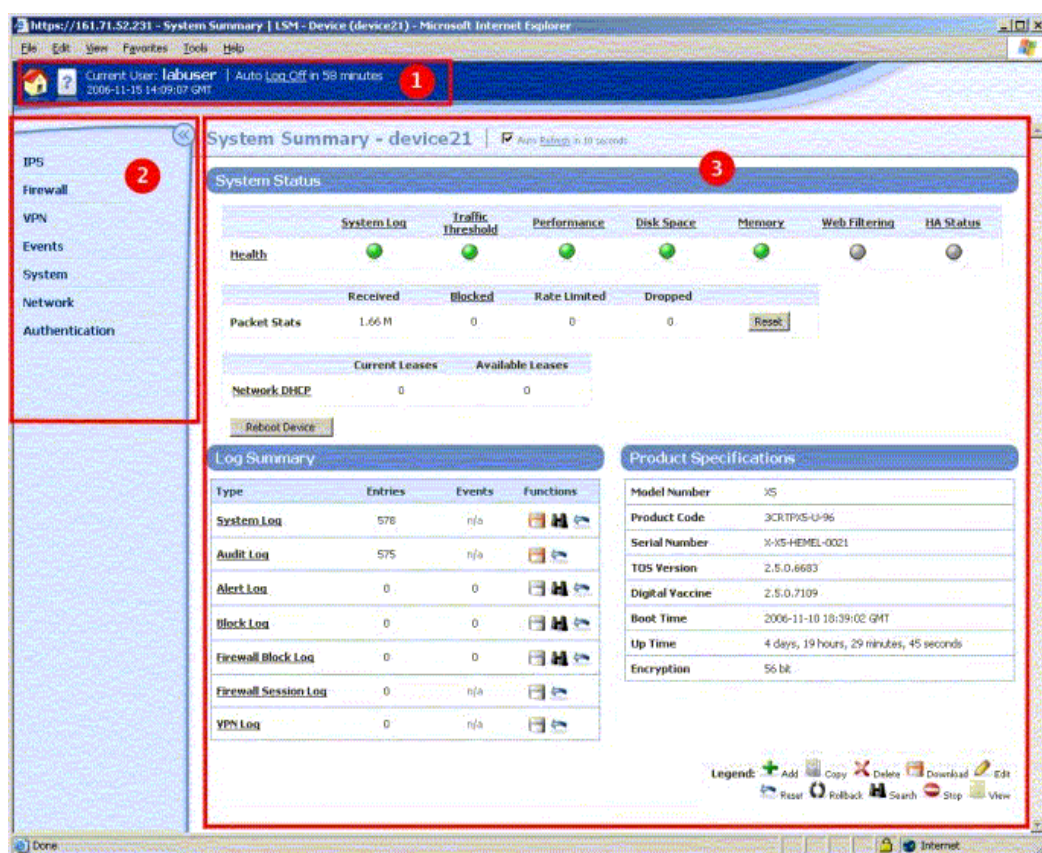
Note Only 10 Web client and 10 SSH (for CLI) connections are allowed to connect to a device at once.

LSM Screen Layout

The LSM provides features in two main areas of the browser window:

- **Main Menu Bar** — Located at the top of the browser window (see item 1 in the figure). This area provides quick access to the System Summary page, online help, and current user and device status.
- **Navigation** — Located on the left side bar of the browser window (see item 2 in the figure). The Navigation bar provides access to the LSM menu functions. To view all the options available for a main menu item (IPS for example), click the menu label. On an expanded menu, options with a + indicate that additional sub-menu are available. When you select a menu item, the content and functionality area displays the content and available options. If you click the << icon in the upper right corner of the Navigation menu, the menu collapses to provide more screen space for the current page displayed in the Content and Functionality area. Click >> to re-open the menu.
- **Content and Functionality** — Located on the right side of the browser window (see item 3 in the figure). This area displays pages from which you can monitor the device operation and performance, view current configuration settings, and modify configuration. The content updates when you click a link in the LSM menu, or when you select buttons or links within a page. Links may display new content or open dialog boxes. When you first log onto the LSM, the [System Summary](#) page automatically displays in this area.



Figure 2-2: LSM Screen Layout



Main Menu Bar

The dark blue bar at the top of the LSM screen provides quick access to basic logon information. The following table lists the available options in the Main Menu Bar:

Table 2–1: Main Menu Bar Options

Option	Description
System Summary 	To display the System Summary, click the System Summary icon. For information about this page, see “System Summary” on page 12 .
Online Help 	To access the X family online help, click the Launch Help Window icon.
Current User	Displays the login name for the current user.
Current date and time	Displays the current date and time on the X family device. The date and time settings on the device are determined by the time synchronization method and time zone configured for the device. For details, see “Time Options” on page 229 .
Auto Log Off	To log off of the LSM, click the Log Off link. For security purposes, LSM sessions have a timeout period. This timeout period determines how long the LSM can remain idle before automatically ending the session/ logging off the user. The default timeout period is 60 minutes. LSM administrators with super-user access can change the default timeout period from the Preferences page (Authentication > Preferences). For details, see “Preferences” on page 266 .

Navigation

You can access the available features of the LSM by selecting an option from the navigation area. The LSM displays the page you select in the content and functionality area of the browser. Each option list displays a tier of links and features for maintaining and monitoring the device

The following table lists the available options in the navigation area:

Table 2–2: Navigation Options

Option	Description
IPS	<ul style="list-style-type: none"> • Create and manage security profiles used to monitor traffic between security zones. This includes reviewing category settings, creating filter overrides, and specifying limits and exceptions for user-specified IP address. • Create and manage traffic threshold filters, action sets, and ports for IPS services. • Manage and configure settings for IPS filters, the Threat Suppression Engine (TSE), and global Adaptive Filter. <p>See “Chapter 3, “IPS Filtering” for more information.</p>
Firewall	<ul style="list-style-type: none"> • View and configure settings for the firewall. • View and configure web filtering for the web filter service and create a custom filter list to permit or block traffic based on user-specified URLs. <p>See Chapter 4, “Firewall” for more information.</p>
VPN	View, configure and manage settings for site-to-site and/or client-to-site VPN connections. See Chapter 7, “VPN” for more information.
Events	<ul style="list-style-type: none"> • View, download, print, and reset Alert, Audit, Block, and System logs. • View graphs reporting on traffic flow, traffic-related events, and statistics on firewall hit counts and triggered filters (attack, rate limit, traffic threshold, quarantine and adaptive filter). • Monitor, search, and maintain traffic streams for adaptive filtering, blocked streams, and rate-limited streams. Manually quarantine an IP address or release a quarantined IP address. • View reports on traffic flow, traffic-related events, and statistics on firewall hit counts and triggered filters (attack, rate limit, traffic threshold, quarantine and adaptive filter). • View the status of hardware components, performance (throughput), and system health. <p>See Chapter 5, “Events: Logs, Traffic Streams, Reports” for more information.</p>
System	<ul style="list-style-type: none"> • Configure system controls such as time options, SMS/NMS interaction, and High Availability. • Download and install software and Digital Vaccine (filter) updates. <p>See Chapter 8, “System” for more information.</p>

Table 2–2: Navigation Options (Continued)

Option	Description
Network	<ul style="list-style-type: none"> • Configure network ports, security zones, IP interfaces, IP Address Groups, the DNS server, the default gateway, routing, and DHCP server information. • Access network tools for DNS lookup, find network path, traffic capture, ping, and trace route functionality. See Chapter 6, “Network” for more information.
Authentication	Create, modify, and manage user accounts. Configure authentication. See Chapter 9, “Authentication” for more information.

Content and Functionality

The LSM displays all data in the central area of the browser window. As you browse and select linked options from the navigation area, pages display allowing you to review information, configure options, or search data. Links selected on these pages may display additional pages or dialog boxes depending on the feature selected.

Title Bar

On each page, you can see the position of the page in the menu hierarchy provided in the title bar. For example, on the Alert Log page, the menu hierarchy indicates that the page is located off the **EVENTS > LOGS** sub-menu. On tabbed menu pages, you can navigate up the hierarchy from the current location by clicking on the link in the hierarchy listing.

Auto Refresh

Some pages (such as System Summary) automatically refresh themselves periodically.

- To disable the auto refresh function, deselect the **Auto Refresh** check box.
- To manually refresh: click the **Refresh** link.
- To reconfigure the **Page Refresh Time**, see [“Preferences” on page 266](#).

Tabbed Menu Options

Some sub-menu options previously available in the left-hand navigation menu are now accessible as a tab on the main page for the menu. For example, from the Tools page, the following tabs are available: **DNS Lookup**, **Find Network Path**, **Traffic Capture**, **Ping**, and **Traceroute**.

System Summary

The System Summary page automatically displays when you first log onto the LSM. To redisplay the System Summary page at any time, click the **System Summary** icon, in the [Main Menu Bar](#).

The System Summary page includes the following:

- [System Status](#) — Displays summary information about the device health, packet statistics, and network DHCP. Also provides access to the **Reboot Device** function.
- [Log Summary](#) — Displays summary information about all the Event Logs.
- [Product Specifications](#) — Displays product, version, time, and encryption information.

System Status

Health

The **Health** section of the Statistics frame displays a color indicator of the hardware health of the device. For detailed information about each of the health indicators, click on the corresponding link above the color indicator. The **Health** section includes indicators for the following components:

- **System Log**
- **Traffic Threshold**
- **Performance**
- **Disk Space**
- **Memory**
- **Web Filtering**
- **HA Status**

The colors indicate the current state of each component:

- Green if there are no problems
- Yellow if there is a major warning
- Red if there is a critical warning
- Grey if the service is disabled

You can set the thresholds for warnings. This defines when the indicator color will change based on the usage of those components. For more information, see [“Thresholds to Monitor Memory and Disk Usage” on page 239](#), and select **System > Thresholds** in the Navigation area.

If the System Log is other than green, you can click on the indicator to view the error that caused the condition.



Note When you view the logged error, the indicator resets and changes to green under **System Summary**.

Packet Stats

The Packet Stats section provides basic traffic statistics including the following:

- **Received** — Total number of packets received and scanned by the Threat Suppression Engine
- **Blocked** — Total number of packets that have been blocked by the Threat Suppression Engine
- **Rate Limited** — The number of packets that matched a filter configured to a permit action set
- **Dropped** — Total number of packets that have been dropped because they are not properly formed or formatted

To reset the counters, click the **Reset** link.

Packet counters provide a snapshot of the traffic going through your network. The packet totals give a partial account of blocked activity according to the filters. All other filter results affect the packet totals.



Note The counters are not synchronized with each other; packets may be counted more than once in some situations.

The counters display the amount of packets tracked. If the number is less than 1M, the Packet Statistics section displays the full amount. If the amount is greater than 999,999 K, the information is abbreviated with a unit factor. For example, 734,123K would display fully whereas 4,004,876,543 displays as 4.00B. When the number reaches the million and billion mark, the number displays as a decimal amount with a letter (such as G for gigabytes). The unit factors include, M for mega, G for giga, and T for tera. To view the full amount, hover your mouse over the displayed amount. A Tool Tip pops up, displaying the full packet amount.

Network DHCP

The Network DHCP section displays the following information:

- Current Leases
- Available Leases

Reboot Device

To reboot the device, click the **Reboot Device** link

Log Summary

The **Log Summary** section displays the number of entries and events for each type of Event Log. In addition, it allows you to perform functions on those logs.

- **System Log**
- **Audit Log**. This log is only available to those with Super User access.
- **Alert Log**
- **Block Log**
- **Firewall Block Log**
- **Firewall Session Log**
- **VPN Log**

For more detailed information about these logs, select **Events > Logs**.

Product Specifications

The Product Specification section displays the following information:

- **Model Number** — Model number of the device.
- **Product Code** — The device product code.
- **Serial Number** — Serial number of the device.
- **TOS Version** — Version number of the TOS software.
- **Digital Vaccine** — Version number of the Digital Vaccine.
- **Boot Time** — Time when the device was last started.
- **Up Time** — How long the device has been operating continuously.
- **Encryption** — Current encryption method being used. By default all new X family devices are supplied with 56-bit DES encryption only. To enable strong encryption functionality (3DES, 128-AES, 192-AES, 256-AES), install the correct Strong Encryption Service Pack for your device. You can download encryption service packs from the TMC Web site.

3 IPS Filtering

LSM Navigation describes the LSM interface, how to log in, and the general sections of the application.

Overview

The X family provides the TippingPoint™ Intrusion Prevention System (IPS) with Digital Vaccine (DV) filters that can be used to police your network to screen out malicious or unwanted traffic such as:

- Vulnerability Attacks and Exploits
- Worms
- Spyware
- Peer-to-Peer applications

In addition to the Digital Vaccine filters, the IPS function also provides **Traffic Threshold** filters you can use to profile and shape network bandwidth.

All IPS filtering occurs inline on traffic that has been permitted through the X family firewall. Filtering is performed by the **Threat Suppression Engine**, custom software designed to detect and block a broad range of attacks at high speed. When a packet matches an IPS filter, the X family device handles the packets based on the **Action** configured on the filter. For example, if the action set is *Block*, then the packet is dropped. The X family device provides default actions to block or permit traffic with options to quarantine or rate-limit traffic and to notify users or systems when an action executes. Logging options are also available so you can review the types of traffic being filtered by the device. You can customize the default Actions, or create your own based on your network requirements.

A **Security Profile** defines the traffic to be monitored and the DV filters to be applied. Traffic monitoring is based on security zone pairs. For example, to create a Security Profile to monitor traffic coming from the WAN zone to the LAN zone, you select the security zone pair WAN ==> LAN. Then, you can configure the DV filters to apply to that zone. The security zone pair specifies both the zone and the traffic direction which allows you to define separate Security Profiles for traffic in and out of a zone.

The default security profile is set to the ANY ==> ANY security zone pair with all IPS filters configured with the default Digital Vaccine settings. With the default profile in place, all incoming and outgoing traffic in any security zone configured on the device is monitored according to the recommended IPS filter configuration. You can edit the default Security Profile to customize the security zones that it applies to and create custom filter settings, or create your own Security Profiles as required.



Note Before creating Security Profiles, verify that the Network and System configuration on the X family device is set up correctly for your environment. In particular, you need to configure all required Security Zones before you can create the Security Profiles to protect them. For details, see [“System” on page 217](#) and [“Network” on page 129](#).

You can monitor and configure IPS from the IPS menu pages available in the LSM. For additional information, see the following topics:

- [“Using the IPS” on page 16](#)
- [“Security Profiles” on page 17](#)
- [“IPS Digital Vaccine \(DV\) Filters” on page 23](#)
- [“Traffic Threshold Filters” on page 38](#)
- [“Action Sets” on page 44](#)

Using the IPS

You can monitor and configure the settings for IPS from the IPS menu pages available in the LSM. The following menu options are available:

- **Security Profiles** — View and manage the Security Profiles available on the device, view the security profile coverage by security zone.
- **Traffic Threshold** — View, manage and create Traffic Threshold filters to monitor network traffic levels. These filters can be configured to trigger when traffic is either above or below normal levels.
- **Action Sets** — View, manage and create actions that define the operations a filter performs when a traffic match occurs.
- **IPS Services** — Add and manage non-standard ports supported by the device. Use this feature to configure additional ports associated with specific applications, services, and protocols to expand scanning of traffic. When filters scan traffic against the standard ports for listed services, the engine then accesses and scans traffic against the list of additional ports.
- **Preferences** — Reset IPS filters to the factory default values, configure timeout, logging, and congestion threshold settings to manage performance of the Threat Suppression Engine, configure the Adaptive Filter feature used to protect performance from the effects of over-active filters.

For details on each menu option, see the following topics:

- [“Security Profiles” on page 17](#)
- [“Traffic Threshold Filters” on page 38](#)
- [“Action Sets” on page 44](#)
- [“IPS Services” on page 55](#)
- [“Preferences” on page 57](#)

Security Profiles

On the X family device, **Security Profiles** are used to apply DV filter policies. A Security Profile defines the traffic to be monitored based on security zones (for example, ANY ==> ANY, LAN ==> WAN, or WAN ==> LAN) and the DV filters to be applied.

A Security Profile consists of the following components:

- **Identification** — Profile name and description.
- **Security Zones** — Specifies the incoming and outgoing security zones to which the Security Profile applies.
- **IPS Filter Category Settings** — Determines the State and Action that applies to all filters within a given Filter Category group.
- **Filter overrides** — Configure filter-level settings that override the Category Settings (optional.)
- **Global Limits and Exceptions** — Configure settings to apply filters differently based on IP address. You can limit filters to apply only to traffic between a source and destination IP address or address range, or apply filters to all traffic except the traffic between specified source and destination IP addresses or address ranges.

When a Security Profile is initially created, the recommended settings for all filter categories are set.

Default Security Profile

The default security profile is set to the ANY ==> ANY security zone pair with all IPS filters configured with the default Digital Vaccine settings. With the default profile in place, all incoming and outgoing traffic in any security zone configured on the device is monitored according to the recommended DV filter configuration. You can edit the default Security Profile to customize the security zones that it applies to and create custom filter settings, or create your own Security Profiles as required. We recommend that you keep the default Security Profile settings configured for the Security Zone pair ANY ==> ANY. This configuration ensures that all traffic will be inspected by the IPS using the default Security Profile if the traffic does not match a more specific security zone configuration.

Applying Security Profiles to Traffic

Using IPS, it is possible for a packet to match more than one Security Profile depending how the security zone pairs are configured within each profile. As a general rule, the X family device will apply the filtering rules specified in the Security Profile that has the most specific Security Zone pair defined. To determine specificity, the device always considers the incoming zone first. See the following examples to see how the device applies filtering rules when a packet matches more than one Security Profile.

Example 1: Security Profile Zone Configuration

Security Profile	Applies To Security Zone Pair
#1	ANY ==> ANY
#2	LAN ==> WAN

In Example 1, a packet going from the LAN zone to the WAN zone matches both Security Profile #1 and #2. The X family device applies the filtering rules from Security Profile #2 to the packet because the LAN zone is more specific than the ANY zone.

Example 2: Security Profile Zone Configuration

Security Profile	Applies To Security Zone Pair
#4	ANY ==> ANY
#5	ANY ==> WAN
#6	LAN ==> WAN

In Example 2, a packet going from the LAN zone to the WAN zone matches Security Profiles #4, #5 and #6. However, the X family device applies filtering rules from Security Profile #6 to the packet because the LAN zone is more specific than the ANY zone.

For additional information on Security Profiles, see the following topics:

- [“Managing Security Profiles” on page 19](#)
- [“Configuring DV Filters” on page 25](#)
- [“Configure Filter Limits/Exceptions based on IP Address” on page 34](#)

Managing Security Profiles

Use the Security Profiles page (**IPS > Security Profiles**) to create and manage the Security Profiles used to apply IPS filtering to security zone traffic.

Figure 3–1: Security Profiles Page




The following table provides a summary of tasks available to configure and manage security profiles from the Security Profiles menu pages in the LSM.

Table 3–1: Security Profile Tasks

Task	Procedure
View all Security Profiles	<p>From the LSM menu, select IPS > Security Profiles. Then, click a Security Profile name to open the profile. You can view a list of the Security Profiles as well as a listing that shows which Security Profiles provide DV filtering for the different Security Zones configured on the device.</p> <p>Note You cannot delete the default Security Profile.</p>
Create a Security Profile	From the LSM menu, select IPS > Security Profiles . On the Security Profile page, click Create .
Edit a Security Profile	From the LSM menu, select IPS > Security Profiles . On the Security Profile page, click Edit .
Delete a Security Profile	On the Security Profiles page, click X . When you delete the profile, all the global and filter level settings are deleted.
Change category settings for a group of filters	On the Edit Security Profile page in the Profile Details (Advanced) section, change the State and Action setting for the category you want to modify. Then, Save the updated profile.

Table 3–1: Security Profile Tasks (Continued)

Task	Procedure
Override global filter settings (create filter level settings)	On the Edit Security Profile page in the Profile Details (Advanced) Filters section, click Search Filters . On the Search Filters page, locate the filter to override. Click the + icon to add the filter to the Security Profile. Then, edit the filter to customize the settings.
Restore filter to global category settings (Delete filter override)	On the Edit Security Profile page in the Profile Details (Advanced) Filters section, locate the filter override to delete. Then, click  .
Edit Port Scan/Host Sweep Filters	The Port Scan/Host Sweep filters are a special type of filter used to protect the network against Port Scan/Host Sweep attacks. These filters can only be applied to Security Zones that include physical ports. For additional information on these filters, see “Port Scan/Host Sweep Filters” on page 35 .

For additional information, see the following topics:

- [“Security Profile Details” on page 20](#)
- [“Create a Security Profile” on page 21](#)
- [“Edit a Security Profile” on page 22](#)
- [“View DV Filters” on page 26](#)
- [“Edit DV Filter Category Settings” on page 29](#)
- [“Port Scan/Host Sweep Filters” on page 35](#)

Security Profile Details

The following table describes the information available on the Security Profiles page.

Table 3–2: Security Profile Details


Parameter	Description
Current Profiles: This section lists all the Security Profiles currently configured on the X family device.	
Profile Name	The name assigned to the Security Profile. The Default Security Profile is pre-configured on the device. You can customize this profile to add Security Zone pairs or modify global and individual filter settings, but you cannot delete or rename this profile.
Description	Displays the description entered for the Security Profile if any exists.
Function(s) 	The functions available to manage Security Profiles: <ul style="list-style-type: none"> • Edit the Security Profile to configure security zones, Category Settings, filter overrides, or global limits and exceptions • Delete the Security Profile.

Table 3–2: Security Profile Details (Continued)


Parameter	Description
<p>Security Zones: This section lists all the security zone pairs that are currently protected by a Security Profile.</p> <p>Note If a Traffic Threshold has been configured with a Security Zone pair that is not protected by a Security Profile, the pair will be listed in the table in red along with the following message:</p> <p>No security profile is assigned to the security zones. Traffic will NOT be inspected by the IPS.</p> <p>To correct the error, add the security zone pair to an existing Security Profile, or create a new Profile to protect it.</p>	
Incoming	The Security Zone that is the traffic source
Outgoing	The Security Zone that is the traffic destination
Security Profile	The name of the Security Zone configured on the device

For additional information, see the following topics:

- [“Create a Security Profile” on page 21](#)
- [“Edit a Security Profile” on page 22](#)
- [“View DV Filters” on page 26](#)
- [“Edit DV Filter Category Settings” on page 29](#)

Create a Security Profile

STEP 1 On the LSM menu, select **IPS > Security Profiles**. Then, click the **Create Security Profile** button.

STEP 2 On the Create Security Profiles page, click the  (**edit**) icon to edit the desired security profile.

STEP 3 In the **Security Zones** section, specify the security zone pairs for the Security Profile:

STEP A Select the **Incoming** and **Outgoing** Security Zone.

STEP B Click **Add to table**.

Repeat this process until you have added all the required security zone pairs.



Note For additional information about setting up the Security Zones, see [“Security Zone Configuration” on page 135](#).

STEP 4 Review or configure advanced configuration options. If the advanced options are not visible, click **Show Advanced Options**. In the **Profile Details (Advanced)** section in the **Category**


Settings table, change the global State or Action for a filter Category Group if required. For more detailed instructions, see [“Edit Category Settings for a Filter Group” on page 30](#).

STEP 5 Click **Create**.

After you create the Security Profile, you can edit the Security Profile and perform additional advanced configuration to create filter overrides and specify global limits and exceptions.

Edit a Security Profile

STEP 1 On the LSM menu, select **IPS > Security Profiles**.


STEP 2 On the Create Security Profiles page, click the  (**edit**) icon to edit the desired security profile.

STEP 3 In the **Security Zones** section, modify the security zone pair configuration, if necessary.

STEP A Select the **Incoming** and **Outgoing** Security Zone.

STEP B Click **Add to table**.

Repeat this process until you have added all the required security zone pairs.

STEP C Click  to delete a security zone.

STEP 4 Review or configure advanced configuration options. If the advanced options are not visible, click **Show Advanced Options**. Do any of the following as needed:

- In the **Profile Details (Advanced)** section in the **Category Settings** table, change the global State or Action for a filter Category Group if required. For more detailed instructions, see [“Edit Category Settings for a Filter Group” on page 30](#).
- To review filters or add a filter to the Security Profile for customization, locate the filter using the **Search Filters** button or **View all filters** link. For details, see [“Edit Individual Filter Settings” on page 32](#).
- Configure global IP address limits or exceptions if required. For details, see [“Configure Global IP address Limits and Exceptions” on page 34](#).

STEP 5 Click **Save** to update the Security Profile.

For additional information, see the following topics:

- [“View DV Filters” on page 26](#)
- [“Edit DV Filter Category Settings” on page 29](#)
- [“Port Scan/Host Sweep Filters” on page 35](#)

IPS Digital Vaccine (DV) Filters

TippingPoint IPS Digital Vaccine (DV) Filters are used to monitor traffic passing between network security zones. Based on the Security Profiles configured on the device, the X family applies the filters to traffic passing between network security zones. Each Security Profile has its own filter settings. Within a Security Profile, you can modify the filter (recommended) settings for a filter category and, if necessary, customize individual filters based on your network environment and security needs. The following sections provide an overview of the DV filters and the components used to configure them:

- [“About the Digital Vaccine Package” on page 23](#)
- [“Filter Components” on page 24](#)
- [“Categories and Category Settings” on page 24](#)

Categories and category settings are used to configure global settings for all filters within a specified category group.

- [“Filter Override Settings” on page 25](#)

Filter settings are used to override the global settings for individual filters within a category group.

About the Digital Vaccine Package

DV filters are contained in a Digital Vaccine (DV) package. All X family devices have a DV package installed and configured to provide out-of-the-box IPS protection for the network. After setting up the X family device, you can customize the DV filter configuration through the LSM.

The filters within the DV package are developed to protect the network from specific exploits as well as potential attack permutations to address Zero-Day threats. These filters include traffic anomaly filters and vulnerability-based filters. Vulnerability-based filters are designed to protect the network from an attack that takes advantage of a weakness in application software. For viruses that are not based on a specific vulnerability in software, the DV provides signature filters. We deliver weekly Digital Vaccine updates which can be automatically installed on the device (**System > Update**). If a critical vulnerability or threat is discovered, Digital Vaccine Updates are immediately distributed to customers.



TIP In addition to providing a download location for Digital Vaccine packages, the TMC also provides DV product documentation that includes more detailed information about the filters included in the DV package, filter updates, and other related information.

Filter Components

IPS filters have the following components which determine the identity the filter type, global and customized settings, and how the device will respond when the Threat Suppression Engine finds traffic matching the filter:

- **Category** — defines the type of network protection provided by the filter. The category is also used to locate the filter in the LSM and to control the global filter settings using the Category Setting configuration.
- **Action set** — defines the actions that execute when the filter is matched.
- **Adaptive Filter Configuration State** — allows you to override the global Adaptive Filter configuration settings so that the filter is not affected by adaptive filtering (see [“Adaptive Filter Configuration” on page 60](#) for additional information)
- **State** — Indicates if the filter is enabled, disabled, or invalid. If the filter is disabled, the Threat Suppression Engine does not use the filter to evaluate traffic.

Categories and Category Settings

Categories and category settings are used to configure global settings for all filters within a specified category group.

DV Filters are organized into Categories and groups based on the type of protection provided:

- **Application Protection Filters** — defend against known exploits and exploits that may take advantage of known vulnerabilities targeting applications and operating systems. This filter type includes the following sub-categories: *Exploits*, *Identity Theft*, *Reconnaissance* (includes Port Scan/Host Sweep filters), *Security Policy*, *Spyware*, *Virus*, and *Vulnerabilities*.
- **Infrastructure Protection Filters** — protect network bandwidth and network infrastructure elements such as routers and firewalls from attack by using protocols and detecting statistical anomalies. These filter types includes the sub-categories *Network Equipment* and *Traffic Normalization*.
- **Performance Protection Filters** — block or rate-limit traffic from applications that can consume excessive bandwidth, leaving network resources available for use by key applications. This filter type includes the following sub-categories: *IM*, *P2P*, and *Streaming Media*.

These Categories are used to locate filters. *Category Settings* are used to assign global configuration settings to filters within a category. For example, if you want don't want to use any filters to monitor P2P traffic, you can the disable the P2P group in the Performance Protection category. You can configure the following global parameters:

- **State** — determines whether filters within the Category are enabled or disabled. If a category is disabled, all filters in the Category are disabled.
- **Action Set** — determines the action set that filters within a Category will execute when a filter match occurs. If the *Recommended* action set is configured, filters within the category are configured with the settings recommended by the Digital Vaccine team, the group can have different settings.

For the best system performance, we recommend that you use global Category Settings and the Recommended action set for all DV filters. However, in some cases, you may need to override the category settings and recommended action for individual filters due to specific network requirements, or in cases where the recommended settings for a filter interact poorly with your network.

Filter Override Settings

For the best system performance, we recommend that you use global Category Settings and the Recommended action set for all DV filters. However, in some cases, you may need to override the category settings and recommended action for individual filters due to specific network requirements, or in cases where the recommended settings for a filter interact poorly with your network.

Filter override settings specify custom settings to be applied to the filter in the Security Profile. Once a filter has been customized, it is not affected by the global Category Settings that specify the filter State and Action. For details, see [“Edit Individual Filter Settings” on page 32](#).

Configuring DV Filters

You configure filters separately for each Security Profile configured on the X family device. When a profile is initially created, all filters are set to the default Category Settings. You can change the Category Settings for filters or edit individual filters from the Edit Security Profile page in the LSM.

Because of the large number of DV filters available on the device, the LSM provides a search interface to view and edit filters. For instructions on using this interface and on editing filters, see the following topics:

- [“View DV Filters” on page 26](#)
- [“Edit DV Filter Category Settings” on page 29](#)
 - [“Edit Category Settings for a Filter Group” on page 30](#)
 - [“Edit Individual Filter Settings” on page 32](#)
 - [“Configure Filter Limits/Exceptions based on IP Address” on page 34](#)
 - [“Edit a Port Scan/Host Sweep Filter” on page 36](#)
- [“Reset an Individual Filter” on page 35](#)

View DV Filters

You can view and manage filters configured for a Security Profile using either the Filters and Filter Search pages. Both pages can be accessed from the Advanced Options Filters section of the Security Profile pages.

- To access the Filters page, use the **View all filters** link
- To access the Filter Search page, click **Search Filters**

The following figure shows the Filters page:

Figure 3–2: IPS: Filters Page with Search

IPS >> PROFILES >> Filters

Keyword(s) ☐ Include Description

Filter # Filter State Filter Control

Categories: Any, Exploits, Identity Theft, IM

Action Set: Any, Recommended, Block, Block + Notify

Protocol: Any, ICMP, TCP, UDP

Severity: Any, Low, Minor, Major

Search >>

Filters List

Legend: + Add to Profile

<input type="checkbox"/>	Filter Name	Control	Action	State	Function(s)
<input type="checkbox"/>	0089: IP: Short Time To Live (1)	Category Settings			+
<input type="checkbox"/>	0121: Stacheldraht: Agent Finder Gaa Scanner (General)	Category Settings		Enabled	+
<input type="checkbox"/>	0262: HTTP: eEye IIS_idg/ida TCAPT Vulnerability Scanner	Category Settings		Enabled	+

You can complete the following tasks from these pages:

- View current filters
- Sort the filter list
- Locate a filter or group of filters
- Add a filter to the filter override list for the current Security Profile
- View the filter description page which includes information about the filter, recommended settings, and the current filter state
- Add or remove a filter from selected Security Profiles

For additional information, see the following topics:

- [“Filter Search” on page 27](#)
- [“Filters List \(All Filters\)” on page 27](#)
- [“Reset an Individual Filter” on page 35](#)
- [“Port Scan/Host Sweep Filters” on page 35](#)

Filter Search

Filter search provides options to view all filters or only those matching user-specified search criteria. You can access the Filter Search page by clicking the Search Filters button when you are editing a Security Profile (IPS > **Security Profiles**, then edit a profile).

You can sort filter search results by filter name, control type, action, or state by clicking a column heading in the **Filters List** table. The search is a string search is is not case sensitive.

The following table describes the available search criteria that can be configured:

Table 3-3: Search Filter Criteria Parameters

Parameter	Description
Keywords	Type a word or phrase to search for in the filter names. The keyword Filter Search is a string search, not a boolean search. You can search for a specific filter number, or for a specific substring in the filter name. If you enter more than one word, the search will look for the exact phrase entered, not a combination of words. For example, if you enter "ICMP reply" the search will not return a filter whose description is "ICMP: Echo Reply."
Include Description	Check this option to search for the specified keyword(s) in the filter descriptions, as well as in the filter names.
Filter #	Search by filter number, type the filter number in this field.
Filter State	Search by current operating state, select from the following: Any, Disabled, or Enabled.
Filter Control	Search for filters configured with Category Settings or filters that have been customize (override).
Categories	Search by IPS filter Category group. Selection list includes all groups in the Application Protection, Infrastructure Protection, and Performance Protection categories.
Action Set	Search by Action Set assigned to filter. The selection list includes all the default and custom Action Sets configured on the device.
Protocol	Search by transport protocol that the filter applies to: ANY, ICMP, TCP, and UDP
Severity	Search by the Severity Level assigned to the filter.

For details on performing a filter search see the following topics:

- [“View Filters with Recommended \(Default\) Settings” on page 29](#)
- [“View Filter Overrides and Custom Settings” on page 29](#)


Filters List (All Filters)

The Filters List page provides a listing of all filters configured for the Security Profile. You can access the page by selecting the **View all filters** link when you are editing the Security Profile. Because of the large number of filters, it may take some time for the device to display the page.

Filter List Details

The following table describes the information and functions available on the Filters List page.


Table 3–4: Filter List Details

Parameter	Description
Search Interface	For details on the search criteria fields, see “Search Filter Criteria Parameters” on page 27 .
Check Box	<p>Use the check box for a filter entry to select it for editing. After checking the desired filters, use the Add Selected Filters button to add the filters to the Security Profile so you can edit them.</p> <p>If a filter entry has no check box, that filter has already been added to the Security Profile. You can manage these filters from the Security Profiles page Filters table.</p>
Filter Name	<p>The name of the filter. The name contains the filter number and additional information relating to the protocol the filter applies and/or other descriptive information about the purpose of the filter (<i>0079: ICMP:Echo Reply</i>). These names are assigned by the Digital Vaccine team.</p> <p>To view filter information, click the name of the filter.</p>
Control	<p>Indicates whether the filter configuration is:</p> <ul style="list-style-type: none"> • Category Settings — uses the global Category Settings configured for the filter’s category. To view the Category and Category Group for filter, click the filter name. • Filter — uses custom settings configured from the Security Profile page. You can manage customized filters from the Filters table on the Security Profile page.
Action Set	<p>Indicates the action set currently assigned to the filter. If the filter uses Category Settings and the Action Set is recommended, the Action field lists Disabled to indicate that the filter is under the control of the default configuration.</p> <p>If the filter has an override, the Action selected in the override is displayed.</p>
State	Indicates whether the filter is enabled (in use) or disabled.
Function(s) 	<p>Available functions for the filter:</p> <ul style="list-style-type: none"> • Add to Security Profile so you can edit the filter settings. <p>If the filter has been overridden, the Add function is not available. You can edit the filter settings from the Filter Override list on the Security Profile page.</p>

For details on viewing filters on the Filter List page, see the following topics:

- [“View Filters with Recommended \(Default\) Settings” on page 29](#)
- [“View Filter Overrides and Custom Settings” on page 29](#)

View Filters with Recommended (Default) Settings

- STEP 1** On the LSM menu, select **IPS > Security Profiles**.
- STEP 2** On the Security Profiles page, click the  (**edit**) icon to edit the desired security profile.
- STEP 3** On the Edit Security Profile page, if the **Profile Details (Advanced)** table is not visible, click **Show Advanced Options**.
- STEP 4** In the **Profile Details (Advanced)** table, scroll down to the Filters section. You can click either **View all filters** or **Search Filters**.
- **View all filters** displays the Filters page. Because of the large number of filters, this action may take some time to execute.
If you select this option, the Search Filters page displays a list of the available IPS filters. You can sort the filters by filter name, control type, action, or state by clicking the appropriate column heading in the Filters List table. To specify new search criteria, use the search interface available at the top of the page.
 - **Search Filters** displays the Search Filters page so you can specify filter search criteria and perform the search.
If you select this option, select the desired Search criteria. Then click **Search**. Note that the Search facility performs string searches. If you select **Search Filters**, the Search Filters page displays with only the search interface displayed. To locate filters, specify one or more search parameters. Then, click **Search**. Note that the search is a string search.

View Filter Overrides and Custom Settings

- STEP 1** On the LSM menu, select **IPS > Security Profiles**.
- STEP 2** On the Security Profiles page, click the **Profile Name** you want to edit.
- STEP 3** On the Edit Security Profile page, if the **Profile Details (Advanced)** table is not visible, click **Show Advanced Options**.
- STEP 4** In the **Profile Details (Advanced)** table, scroll down to the **Filters** section.
In the Filters section, the table lists all filters that have been added to the Profile.
- STEP 5** To view and/or edit a filter, click the **Filter Name**.
If you want to remove the filter override and return the filter to its default, recommended settings, click the **Delete** icon.

Edit DV Filter Category Settings

By default, a Security Profile uses the Category Settings for all filters available in the Digital Vaccine package. In some cases you may not need a particular filter or category of filters. For example, you may want to disable filters that protect a particular type of web server against attack if that server is not

installed on your network. From the LSM, you can modify the filter configuration for a Security Profile by category or by changing individual filter settings. You can make the following types of changes:

- Edit a Filter Category Group to enable/disable all filters in the group or change the assigned action for all filters in the group.
- Edit an individual filter or group of filters to modify the following settings: State, Action, Adaptive Filter Configuration State, Exceptions.

When you edit a filter, the changes only affect the Security Profile in which you make the edits. This allows you to have different filter configurations for different Security Zones.

For details on editing filters, see the following topics:

- [“Edit Category Settings for a Filter Group” on page 30](#)
- [“Edit Individual Filter Settings” on page 32](#)
- [“Edit a Port Scan/Host Sweep Filter” on page 36](#)



Note If the category setting is enabled and you disable the filter, the filter may still display as enabled.

Edit Category Settings for a Filter Group



Note When you change the Category Settings for a group of filters, the settings will not affect any filters that have been customized (overridden). Filters that have been customized display on the Edit Security Profiles page in the Filters section. On the Filters List page, these filters are listed with Control = Filter.

- STEP 1** From the LSM menu, click **Security Profiles**.
- STEP 2** On the Security Profiles page in the **Current Profiles** table, click the **pencil** icon for the Security Profile you want to change.
- STEP 3** On the Edit Security Profile page in the **Advanced Options** section, locate the Filter Category group in the **Category Settings** table.

The following figure shows the Category Settings table.

Figure 3–3: Edit Security Profile Page - Advanced Options - Category Settings

Category Name	Filter Name	State	Action
Application Protection	Exploits	<input checked="" type="checkbox"/> Enabled	Recommended
	Identity Theft	<input checked="" type="checkbox"/> Enabled	Recommended
	Reconnaissance	<input checked="" type="checkbox"/> Enabled	Recommended
	Security Policy	<input checked="" type="checkbox"/> Enabled	Recommended
	Spyware	<input checked="" type="checkbox"/> Enabled	Recommended
	Virus	<input checked="" type="checkbox"/> Enabled	Recommended
	Vulnerabilities	<input checked="" type="checkbox"/> Enabled	Recommended
Infrastructure Protection	Network Equipment	<input checked="" type="checkbox"/> Enabled	Recommended
	Traffic Normalization	<input checked="" type="checkbox"/> Enabled	Recommended
Performance Protection	IM	<input checked="" type="checkbox"/> Enabled	Recommended
	P2P	<input checked="" type="checkbox"/> Enabled	Recommended
	Streaming Media	<input checked="" type="checkbox"/> Enabled	Recommended

Click **Show Advanced Options** if the **Advanced Options** table is not displayed.

STEP 4 Modify the settings as required:

- In the **State** field for the Category group, clear the check box to disable all filters in the group, or check it to enable all filters in the group.
- In the **Action** field, select the Action Set to be used for *all* filters in the group.

The Recommended Action Set is the system default for all category groups. If this action is selected, each filter in the group is configured with the recommended settings. Filters within the group may have different settings for *State* and *Action*.

The following action set selections are available for each Filter Category:

- For all **Application Protection** filters, the selection list includes all available actions sets.
- For **Infrastructure Protection** filters, the selection list includes all available actions sets.
- For **Performance Protection** filters, the selection list includes all available block action sets.

STEP 5 After making the desired changes, click **Save** (at the bottom of the Security Profile page).

Edit Individual Filters to Override Category Settings

For the best system performance, we recommend that you use global Category Settings and the Recommended action set for all DV filters. However, in some cases, you may need to override the category settings and recommended action for individual filters due to specific network requirements, or in cases where the recommended settings for a filter interact poorly with your network.

Filter override settings specify custom settings to be applied to the filter in the Security Profile. Once a filter has been customized, it is not affected by the global Category Settings that apply to all other filters in the category group. For details, see [“Edit Individual Filter Settings” on page 32](#).

Edit Individual Filter Settings



Note These instructions are for editing all Application Protection, Infrastructure Protection, and Performance Protection filters with the exception of the Port Scan/Host Sweep filters available in the Application Protection: Reconnaissance category. For details on Port Scan/Host Sweep filters, see [“Port Scan/Host Sweep Filters” on page 35](#).

- STEP 1** From the LSM menu, click **Security Profiles**.
- STEP 2** On the Security Profiles page in the **Current Profiles** table, click the **pencil** icon for the Security Profile you want to change.
- STEP 3** On the Edit Security Profile page in the **Advanced Options** section, locate the **Filters** table.
- STEP 4** In the **Filters** table, find the filters that you want to edit. Do one of the following:
- Click **Search Filters**. Then, on the Search Filters page, specify the search criteria. Click **Search** to display the filter search results.
 - Click **View all filters** to display the Filters page with all IPS filters available.
- Because of the large number of IPS filters, this operation may take a few moments to complete.
- STEP 5** To view filter details including filter name description and default settings, click the filter name to display the details on the View Filter page.

IPS >> PROFILES >> FILTER SEARCH >>
View Filter

IPS

- Security Profiles
- Traffic Threshold
- Action Sets
- IPS Services
- Preferences

Firewall

VPN

Events

System

Network

Authentication

General Information

Filter Name	0027: IP Options: Record Route (RR)
Category	Infrastructure Protection - Network Equipment Protection
Severity	Minor
Description	This filter detects the Record Route option (option number 7).

IP options are rarely used by valid software applications, but are often used by attackers for malicious purposes. In general, any packets that carry IP options should be viewed as suspicious and should be denied at the firewall.

References
<http://www.iana.org/assignments/ip-parameters>
<http://www.ietf.org/rfc/rfc0791.txt>

Recommended Disabled

Security Profiles

Add this filter to the following security profiles:

[Check all](#) [Uncheck all](#)

☐ [Default Security Profile](#)

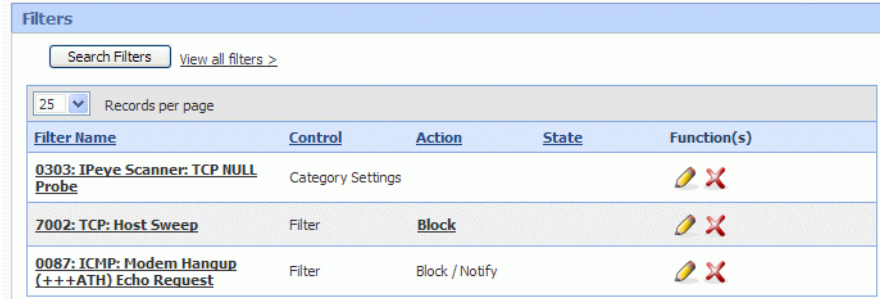
Save **Cancel**







On the View Filter page, you can also add or remove the filter from Security Profiles using the check boxes in the Security Profiles table. After making changes, click **Save**.

STEP 6 In the **Filters List** table, select the filter or filters to edit:

- To select a single filter, click  to add the filter to the Security Profile.
- To select multiple filters, select the check box for each filter. Then, click the **Add Selected Filters** button at the bottom of the Filters page.

The Security Profiles page displays with the selected filters in the **Advanced Options - Filters** table as shown in the following figure.



Filter Name	Control	Action	State	Function(s)
0303: IPey Scanner: TCP NULL Probe	Category Settings			 
7002: TCP: Host Sweep	Filter	Block		 
0087: ICMP: Modem Hangup (+++ATH) Echo Request	Filter	Block / Notify		 

STEP 7 To edit the filter settings, click the filter name, or the **pencil** icon.

STEP 8 On the Edit Filter page in the **Action/State** section, select **Use Category Settings** or **Override**. If you select **Override** to use a different action set for the filter, do the following:

STEP A Select the **Override** radio button in the **Parameters** section.

STEP B Check **Enabled** to enable the filter, or clear the check box if you want to disable the filter.

STEP C Choose an **Action** from the drop-down list.

If the action for the filter is *Recommended* and you do not change it, the filter may remain disabled even when you select the **Enabled** check box. This happens because the recommended setting for the filter state is *disabled*. To enable a filter configured in this manner, you must change the action from *Recommended* to another option.

STEP 9 Optionally, set adaptive filter settings for flow control. In the **Adaptive Filter Configuration State** section, select one of the following:

- **Use adaptive configuration settings** — Applies the global adaptive filter settings
- **Do not apply adaptive configuration settings to this filter** — Removes any global adaptive filter settings for this filter

STEP 10 Optionally, define IP address exceptions for the filter. For details, see [“Configure Filter Limits/Exceptions based on IP Address” on page 34](#).

STEP 11 Click **Save**.

Configure Filter Limits/Exceptions based on IP Address

Limits and exceptions allow you to configure the device so that the filters in a Security Profile can be applied differently based on IP address. For example, you can specify a limit setting so that filters only apply to specified source and destination IP addresses or address ranges. You can configure the following limit and exceptions from the LSM:

- **Filter Exceptions** (specific)— Allow traffic that would normally trigger a filter to pass between specific addresses or address ranges without triggering the filter. Configured from the Filter Edit page, these exceptions apply only to the filter on which they are configured.
- **Limit Filter to IP Addresses** (global) —Only apply filters to traffic between specified source and destination IP address pairs. You can configure IP address limits that apply to all the following filter types: Application Protection, Traffic Normalization, and Network Equipment Protection filters. You can configure separate limits that apply only to Performance Protection filters.
- **Exceptions** (global) — Exclude traffic between specified source and destination IP address pairs. You can configure exceptions for the following filter types: Application Protection, Traffic Normalization, Network Equipment Protection, and Performance Protection filters. These exceptions are global for all specified filters.

If a filter has both global and filter-level exception settings, the Threat Suppression Engine uses the filter-level settings to determine how to apply the filter.

The following sections describe the procedures to configure and delete global limits and exceptions from the Security Profile page.


- [“Configure Global IP address Limits and Exceptions” on page 34](#)
- [“Delete a Global Limit/Exception Setting” on page 35](#)
- Configure filter-level exceptions: [“Edit Individual Filter Settings” on page 32](#)

Configure Global IP address Limits and Exceptions

- STEP 1** From LSM menu, click **IPS**. Then, edit the Security Profile where you want to modify limit/exception settings.
- STEP 2** On the Edit Security Profile page in the **Advanced Options** section, scroll down to the **Limits/Exceptions** table.
- Click **Show Advanced Options** if the **Advanced Options** table is not displayed.
- STEP 3** In the **Limits/Exceptions** section, specify the Application Protection Filter Exclusives (limits) for Application Protection, Traffic Normalization, and Network Protection filters:
- STEP A** Enter the **Source Address**.
- Source and Destination IP Addresses can be entered in CIDR format, as “any” or as *.
- STEP B** Enter the **Destination Address**.
- STEP C** Click **add to table below**.
- STEP D** Repeat this process for each IP address exception required.

- STEP 4** In the **Application Protection Filter Setting Exceptions** section, specify the IP address exceptions for Application Protection, Traffic Normalization, Network Equipment Protection and Performance Protection filters.
- STEP 5** In the **Performance Protection Filter Settings** section, specify IP address limits for Performance Protection filters.
- STEP 6** Click **Apply**.

Delete a Global Limit/Exception Setting


- STEP 1** From LSM menu, click **IPS**. Then, edit the Security Profile where you want to modify limit/exception settings.
- STEP 2** On the Edit Security Profile page in the **Advanced Options** section, scroll down to the **Limits/Exceptions** table.
- Click **Show Advanced Options** if the **Advanced Options** table is not displayed.
- STEP 3** Review the global limit and exception address entries. Click  to delete an entry.
- To delete a filter-level exception, edit the filter. For details, see [“Edit Individual Filter Settings” on page 32](#)
- STEP 4** Click **Apply**.

Reset an Individual Filter

If you have created a filter override in a Security Profile, you can restore the filter to its default settings by deleting the Filter from the Security Profile Filters table.

You can also reset all filters to their factory default settings from the IPS Preferences page. If you do this, all the filters will be set to their recommended state and all action sets, rate limits, and thresholds (other than defaults) will be deleted. You will also lose the Security Profiles you have created along with any custom settings configured on the default Security Profile. For details, see [“Reset Filters” on page 57](#).

Delete a Filter Override

- STEP 1** From the LSM menu, click **Security Profiles**.
- STEP 2** On the Security Profiles page in the **Current Profiles** table, click Profile Name for the profile you want to change.
- STEP 3** On the Edit Security Profile page in the **Advanced Options** section, locate the **Filters** table.
- STEP 4** In the **Filters** table, find the entry for the filter override you want to remove. Then, click .
- The filter is restored to the recommended settings for the category it belongs to.

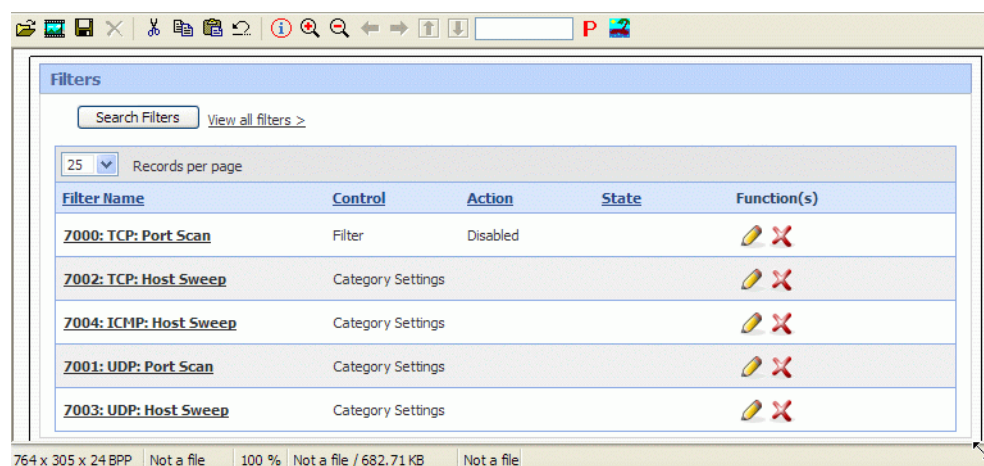
Port Scan/Host Sweep Filters

A port scan attack scans a host looking for any open ports that can be used to infiltrate the network. A host sweep scans multiple hosts on the network looking for a specific listening port that can be used to infiltrate the network.

The Port Scan/Host Sweep Filters (Filter numbers 7000- 7004) available in the *Application Protection Category - Reconnaissance* group are designed to protect the network against these types of attacks. These filters monitor the rate of connections generated by hosts on the network. The filter triggers when the connection rate during a specified interval goes above a given threshold.

The following figure shows the Port Scan/Host Sweep Filters added to the Security Profile for editing.

Figure 3–4: Security Profile: Port Scan/Host Sweep Filter Overrides



The Port Scan/Host Sweep Attack filters can only be used to monitor traffic on Security Zones that include physical ports. That is, you cannot run Port Scan/Host Sweep filters on VLANs or zones configured with a Virtual Server.

In the Category Settings, all Port Scan/Hosts Sweep filters are disabled. To apply these filters to the Security Profile, enable the filters, tune the *threshold* and *timeout* interval settings, and assign an action set based on your network requirements. Because the *Recommended* setting for Port Scan Host/Sweep filters is disabled, you have to assign a specific action to the filter to enable it.

Filter Tuning

You can tune the sensitivity of Port Scan/Host Sweep filters by adjusting their *Timeout* and *Threshold* parameters. The timeout value is used in combination with the threshold value to determine whether or not an alert is sent.

For example, if the time interval is 300 seconds (5 minutes) and the connection threshold is 100 hits, then the filter is triggered every time the rate of connections exceeds 100, or exceeds a multiple of the threshold (101, 201, 301...) within the 300 second (five minute) time period.

The filters support any of the configured action sets available on the device. You can also configure IP address exceptions.

Edit a Port Scan/Host Sweep Filter

STEP 1 From the LSM menu, click **Security Profiles**. Then, edit the Security Profile on which you want to provide Port Scan/Host Sweep filter protection.

The Security Profile must contain zones that have physical ports.

STEP 2 On the Security Profile page, scroll down to the **Advanced Options, Filters** section.

- STEP 3** Locate the Port Scan/Host Sweep filters:
- STEP A** Click **Search Filters**. Then, on the Filter Search page, specify the search criteria:
 - STEP B** In the **Categories** selection list, click **Reconnaissance**.
 - STEP C** In the **Severity** selection list, click **Low**.
 - STEP D** Click **Search**.
 - STEP E** In the Filters List with the search results, click the >> page control button to go to the last page of the results.
- STEP 4** To add the Port Scan/Host Sweep filters to the Security Profile for editing, do one of the following:
- To add an individual filter, click the **Add** icon in the **Functions** column for that filter.
 - To add multiple filters, check each filter. Then, click **Add Selected Filters**.
- STEP 5** On the Edit Security Profile page in the **Filters** section, click the **Filter Name** to edit the settings.
- STEP 6** In the **Action/State** section, select **Use Category Settings** or **Override**. If you select **Override** to use a different action set for the filter, do the following:
- STEP A** Select the **Override** radio button in the **Parameters** section.
 - STEP B** Check the **Enabled** check box.
 - STEP C** Choose an **Action** from the drop-down list.
- STEP 7** Optionally, you can set adaptive filter settings for flow control. In the **Adaptive Filter Configuration State** section, select one of the following:
- **Use adaptive configuration settings** — Applies the global adaptive filter settings
 - **Do not apply adaptive configuration settings to this filter** — The filter will not be monitored by the Adaptive Filter mechanism
- STEP 8** In the **Scan/Sweep Parameters** section, do the following:
- STEP A** Enter the number of seconds for the **Timeout**.
 - STEP B** Enter the number of hits allowed for the **Threshold**.
- STEP 9** Optionally, you can add exceptions to the filter so that the filter will not be used to monitor traffic from specified IP addresses. In the **Exceptions** section, do the following:
- STEP A** Enter the **Source Address**.
 - STEP B** Enter the **Destination Address**.
 - STEP C** Click **add to the table below**.
- STEP 10** Click **Save**.

Traffic Threshold Filters



Note The default X family configuration does not include any Traffic Threshold filters. You must create them based on your network requirements.

Traffic threshold filters alert you and the device when network traffic varies from the norm. The device determines normal traffic patterns based on the network statistics over time. You can set four types of thresholds for each filter:

- **major increase** — Traffic is greatly over the set threshold.
- **minor increase** — Traffic is slightly over the set threshold.
- **minor decrease** — Traffic is slightly below the set threshold.
- **major decrease** — Traffic is greatly under the set threshold.

Thresholds are expressed as a “% of normal” traffic. For example, a threshold of 150% would fire if traffic exceeded the “normal” amount by 50%. A threshold of 60% would fire if the level of traffic dropped by 40% from “normal” amount of traffic.



Note Network traffic rates are inherently erratic and can vary as much as 50% above or below the normal level on a regular basis. When you set up Traffic Threshold filters, avoid setting small variation percentages for minor and major thresholds to prevent the Traffic Threshold filter from triggering too often.

You can configure an action set for each threshold level configured for the Traffic Threshold filter. When the filter triggers, the device executes the action specified for the threshold setting that triggered the filter. You can also configure traffic thresholds to monitor traffic on the network without taking any action. All traffic threshold activity is recorded in the Traffic Threshold report (**Events > Reports > Traffic Threshold**).

Thresholds trigger when the traffic flow is above the *Above Normal* threshold, or below the *Below Normal* threshold by the set amounts. When traffic exceeds a threshold and returns to normal levels, the device executes the action specified for the threshold that triggered the filter and generates an alert. These alerts inform you of the triggered filter, when the thresholds are exceeded and return to normal, and the exceeded amount. After the filter triggers, you must reset it to re-establish it for use in the device. The filter is not disabled, but it does require resetting.



Note A triggered Traffic Threshold filter will not be applied to traffic until you manually reset it.

Traffic Threshold filter events are recorded in the Alert and Block logs (**Events > Logs**), based on the action set specified for the filter. Information on traffic threshold events is also available in the Traffic Thresholds report (**Events > Reports > Traffic Threshold**).

For additional information on managing and configuring Traffic Threshold filters, see the following topics:

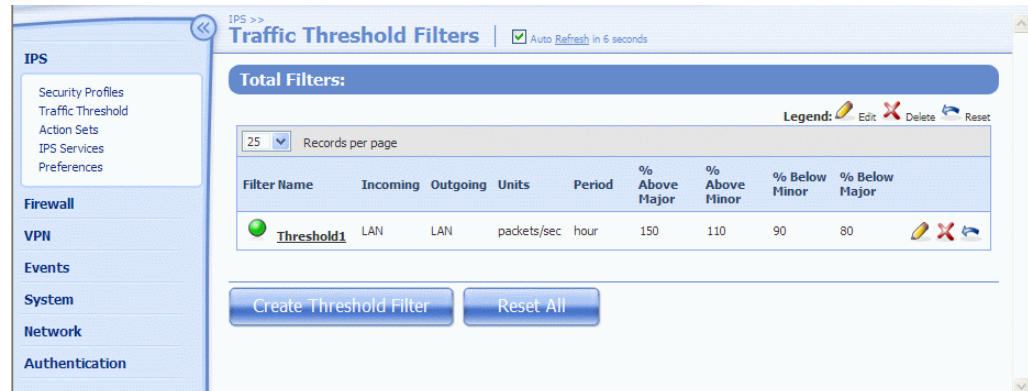
- [“Managing Traffic Threshold Filters” on page 39](#)
- [“Create or Edit a Traffic Threshold Filter” on page 41](#)

Managing Traffic Threshold Filters

You can manage Traffic Threshold filters from the Traffic Threshold Filters page (**IPS > Traffic Threshold filters**).

The following figure shows the Traffic Threshold Filters page.

Figure 3–5: Traffic Threshold Filters Page



You can complete the following tasks from the Traffic Threshold Filters page:

- Create a filter
- Edit a filter
- Reset a Traffic Threshold filter - after a filter triggers, it does not resume monitoring until it is reset.
- Delete a filter

For additional information, see the following topics:

- [“Traffic Threshold Details” on page 39](#)
- [“Create or Edit a Traffic Threshold Filter” on page 41](#)
- [“Traffic Threshold Report” on page 125](#)
- [“Logs” on page 98](#)




Traffic Threshold Details

The following table describes the information and functions available on the Traffic Threshold Filters page.

Table 3–5: Traffic Threshold Filters Details

Column	Definition
Filter Name	Name of the filter
Incoming	The security zone that is the traffic source
Outgoing	The security zone that is the traffic destination

Table 3–5: Traffic Threshold Filters Details

Column	Definition
Units	The number of selected units per second. The unit values include packets, bytes, and connections/second.
Period	The period of time for the historical data. The period values include the last minute, hour, day, 7 days, 30 days, and 35 days.
% Above Major % Above Minor	Major % — Percentage of traffic highly over the threshold Minor % — Percentage of traffic slightly over the threshold
% Below Minor % Below Major	Minor % — Percentage of traffic slightly under the threshold Major % — Percentage of traffic highly under the threshold
Functions	<p>The functions available to manage Traffic Threshold filters:</p> <ul style="list-style-type: none">  • Edit the filter to change configuration parameters.  • Delete the filter.  • Reset the Traffic Threshold filter. After a Traffic Threshold trigger, it cannot resume monitoring until it has been reset.

Create or Edit a Traffic Threshold Filter

Use the Create or Edit Traffic Threshold Filter page to configure the Traffic Threshold filter for your environment. You must create a separate filter for each security zone pair that you want to monitor.

The following figure shows the Create Traffic Threshold Filter page.

Figure 3–6: Create Traffic Threshold Page

IPS >> TRAFFIC THRESHOLD >>
Create Traffic Threshold Filter

Filter Parameters
Traffic threshold filters detect abnormally high or low volumes of network traffic compared to historical baselines. These baselines are continuously monitored and updated.

Filter Name:

Incoming Security Zone: LAN

Outgoing Security Zone: LAN

Units per Second: Packets based on last hour

Monitoring

☒ Monitor only
☐ Monitor with thresholds

Thresholds
Up to 4 thresholds can be configured for each filter: minor increase over normal, major increase over normal, minor drop below normal, and major drop below normal. Each threshold is a percentage change from "normal."

Above Normal

☐ Enabled | Major Threshold % of normal | Action: Permit + Notify
☐ Enabled | Minor Threshold % of normal | Action: Permit + Notify

Below Normal

☐ Enabled | Minor Threshold % of normal | Action: Permit + Notify
☐ Enabled | Major Threshold % of normal | Action: Permit + Notify

Type

☒ Protocol: TCP
☐ Application: TCP Port:

Apply to: ☐ Requests ☐ Replies ☒ Both

Create Cancel

For additional information, see the following topics:

- [“Traffic Threshold Configuration Parameters” on page 42](#)
- [“Configure a Traffic Threshold Filter” on page 43](#)

Traffic Threshold Configuration Parameters

The following table describes the Traffic Threshold filter configuration parameters.

Table 3–6: Traffic Threshold Filters Configuration Parameters

Column	Definition
Filter Name	Name of the filter
Incoming Security Zone Outgoing Security Zone	<p>Select the security zones for the traffic source (incoming) and destination (outgoing). Only zones with a physical port are included in the selection list.</p> <p>Note The security zone pair that you select must be configured on a Security Profile. Otherwise, traffic between the zones is not inspected by IPS and the Security Profile page displays the following message:</p> <p>No security profile is assigned to the security zones. Traffic will NOT be inspected by the IPS.</p>
Units per Second	Select the type of traffic units to track: Packets, Bytes, and Connections . Then, select the period of time for the historical data used to calculate changes in traffic rates: hour, day, 7 days, 30 days, 35 days .
Monitoring	<p>Determines the action for the Traffic Threshold filter. Select one of the following:</p> <ul style="list-style-type: none"> • Monitor only — device generates a Traffic Threshold report without triggering traffic threshold (no alerts are generated) • Monitor with thresholds — when the threshold is triggered, the device performs the action configured for the threshold.
<p>Thresholds:</p> <p>The Thresholds parameters specify the high and low rates that will trigger the filter. Thresholds are expressed as a “% of normal” traffic. For example, a threshold of 120% would fire if traffic exceeded the “normal” amount by 20%. A threshold of 80% would fire if the level of traffic dropped by 20% from “normal” amount of traffic. Also set the state of the filter (enabled/disabled) and the action to perform when the filter triggers.</p>	
Enabled	For each threshold setting, check to enable the threshold. To disable the threshold, clear the check box.
Action	For each threshold setting, select an action to perform when the filter triggers. The action only executes if the Traffic Threshold filter monitoring state is set to Monitor with thresholds .
Above Normal	<p>Major % — Percentage of traffic highly over the threshold</p> <p>Minor % — Percentage of traffic slightly over the threshold</p>
Below Normal	<p>Major % — Percentage of traffic highly under the threshold</p> <p>Minor % — Percentage of traffic slightly under the threshold</p>

Table 3–6: Traffic Threshold Filters Configuration Parameters (Continued)

Column	Definition
Type	<p>Select the traffic protocol or application type of the traffic to be monitored:</p> <ul style="list-style-type: none"> • Protocol — monitor traffic from the selected protocol: TCP, Other, ICMP, and UDP. • Application — monitor traffic for the selected application type on the specified port: TCP or UDP and the Port. <p>Apply to: specify whether the filter monitor tracks requests, replies, or both.</p>
Period	<p>The period of time for the historical data used to calculate the baseline traffic rate: minute, hour, day, 7 days, 30 days, and 35 days.</p>

Configure a Traffic Threshold Filter

- STEP 1** From the LSM menu, select **IPS > Traffic Threshold**.
- STEP 2** On the Traffic Threshold Filters page, click **Create** or click on the name of the Traffic Threshold filter you want to edit.
- STEP 3** On the Create/Edit Traffic Threshold Filters page in the **Filter Parameters** section, type or edit the **Filter Name**.
- STEP 4** Select the traffic source and destination security zones in the **Incoming Security Zone** and **Outgoing Security Zone** drop-down lists.
- STEP 5** In the Units per Second field, select the traffic units you want to track: **Packets**, **Bytes**, or **Connections**. Then, specify the historical time period used to calculate the baseline traffic level to compare against: **minute**, **hour**, **day**, **7 days**, **30 days**, and .
- STEP 6** For **Monitoring**, select an option: **Monitor only** or **Monitor with thresholds**.
The **monitor only** option sets the device to generate a report without triggering traffic thresholds.
- STEP 7** Configure up to 4 threshold parameter settings, state (enable/disable), and action for the filter:
Thresholds settings are specified as a percentage change from the “normal” baseline.
- STEP A** In **Above Normal Major Threshold**, select the **Enabled** check box, enter a percentage amount of normal. Then, select the action to perform when the filter triggers.
- STEP B** For **Above Normal Minor**, select the **Enabled** check box, enter a percentage amount of normal. Then, select the action to perform when the filter triggers.
- STEP C** For **Below Normal Major**, select the **Enabled** check box, enter a percentage amount of normal. Then, select the action to perform when the filter triggers.

STEP D For **Below Normal Minor**, select the **Enabled** check box, enter a percentage amount of normal. Then, select the action to perform when the filter triggers.

STEP 8 Select either the protocol or application **Type** for the traffic to be monitored:

- **Protocol** — Select the type of protocol from the drop-down list, including **TCP**, **Other**, **ICMP**, and **UDP**.
- **Application** — Select the type of application: **TCP** or **UDP**; enter the **Port**. Then, select one of the following to apply the type to: **requests**, **replies**, or **both**.

STEP 9 Click **Save/Create**.

Action Sets

Action Sets determine what the X family device does when a packet triggers a filter. An action set can contain more than one action, and can contain more than one type of action. The types of action that can be specified include the following:

- **Flow Control** — determines where a packet is sent after it is inspected. A *permit* action allows a packet to reach its intended destination. A *block* action discards a packet. A block action can also be configured to *quarantine* the host and/or perform a *TCP reset*. A *rate limit* action enables you to define the maximum bandwidth available for the traffic stream.
- **Packet Trace** — allows you to capture all or part of a suspicious packet for analysis. You can set the packet trace priority and packet trace verbosity for action sets.
 - **Priority** — sets the relative importance of the information captured. Low priority items will be discarded before medium priority items if there is a resource shortage.
 - **Verbosity** — determines how much of a suspicious packet will be logged for analysis. If you choose *full* verbosity, the whole packet will be recorded. If you choose *partial* verbosity, you can choose how many bytes of the packet (from 64 to 1600 bytes) the packet trace log records.
- **Notification Contacts** — indicate the contacts to notify about the event. These contacts can be systems, individuals, or groups.



Note You must create or modify a notification contact before configuring an Action Set that uses the contact. For details, see [“Notification Contacts” on page 52](#).

TCP Reset and Quarantine actions

For Block action sets, you can configure TCP Reset and Quarantine options.

- **TCP reset** allows the device to reset the TCP connection for the source or destination IP when the Block action executes.



Note Globally enabling the TCP Reset option may negatively impact system performance. We recommend using this option for issues related to mail clients and servers on email related filters.

- **Quarantine** allows the device to block packets based on the IP addresses in the packet that triggers the filter. When a filter with a quarantine option triggers, the device installs two blocks: one for the flow (as is normally done with Block actions) and another for the quarantined IP address. In addition to installing the two blocks, the device quarantines the IP address based on the instructions

in the action set. For example, the user can display a Quarantine web page to notify the user of the problem and optionally provide instructions for fixing it, or the action may redirect all traffic from the quarantined IP address to a quarantine server that provides instructions to correct the problem.

Action Set Configurations

The following table describes various Action Set configurations that can be configured on the X family device:

Action Name	Description
Recommended	This is a default Action Set that cannot be modified. When this action set is assigned to a filter, the filter uses the recommended action setting based on the default Category Settings for the filter. The device uses this Action Set to allow filters within the same category to have different configurations. For example, if you set an entire category of filters to recommended, some filters may be disabled while others are enabled; some may have permit actions assigned while others are set to block.
Block (+TCP Reset) (+Quarantine)	Blocks a packet from being transferred to the network. TCP Reset is an option for resetting blocked TCP flows. Quarantine is an option that redirects the host IP to a quarantine page or area to protect the network from being infected or compromised.
Block + Notify (+TCP Reset) (+Quarantine)	Blocks a packet from being transferred and notifies all selected contacts of the blocked packet. TCP Reset is an option for resetting blocked TCP flows. Quarantine is an option that redirects the host IP to a quarantine page or area to protect the network from being infected or compromised.
Block + Notify + Trace (+TCP Reset) (+Quarantine)	Blocks a packet from being transferred, notifies all selected contacts of the blocked packet, and logs all information about the packet according to the packet trace settings. TCP Reset is an option for resetting blocked TCP flows. Quarantine is an option that redirects the host IP to a quarantine page or area to protect the network from being infected or compromised.
Permit + Notify	This is a default Action Set. Permits a packet and notifies all selected contacts of the packet.
Permit + Notify + Trace	This is a default Action Set. Permits a packet, notifies all selected contacts of the packet, and logs all information about the packet according to the packet trace settings

Default Action Sets

The X family device is pre-configured with a collection of default Action Sets. You can edit the default settings for an action set, or create a new one. You cannot delete a default action set. The following actions sets are available:

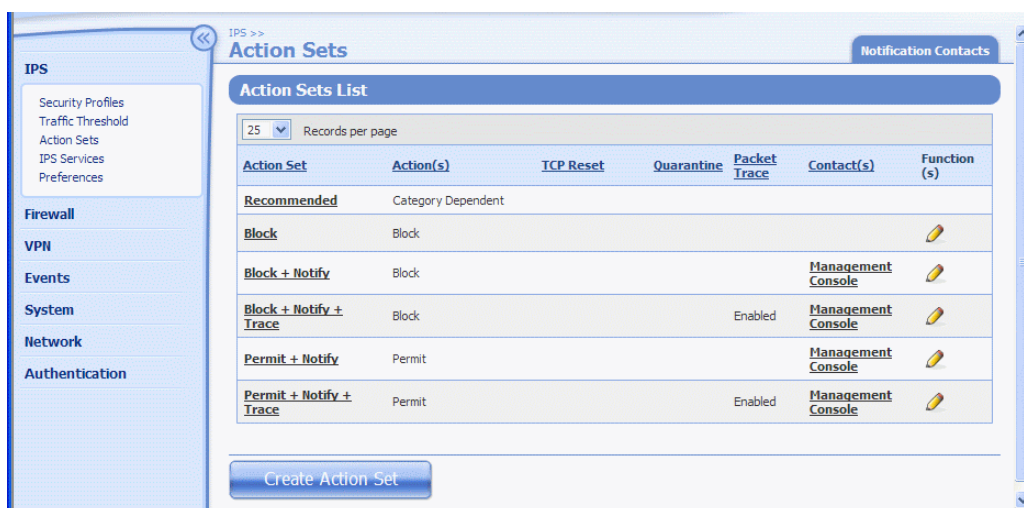
- Recommended
- Block
- Block + Notify
- Block + Notify Trace
- Permit + Notify
- Permit + Notify + Trace

Managing Actions

Use the Action Sets page to review, create and modify Action Sets.

The following figure shows the Action Sets page:

Figure 3–7: IPS: Action Sets Page



You can complete the following tasks from the Action Sets page:

- View and manage existing actions
To sort the Actions listing by characteristics, use the link at the top of each column in the **Action Sets** list table.
- Access the Create and Edit options
- Access the Notification Contacts page to configure contact information

For additional information, see the following topics:

- [“Action Sets Details” on page 47](#)
- [“Configure an Action Set” on page 48](#)
- [“Rate Limit Action Set” on page 49](#)
- [“Quarantine Action Set” on page 49](#)



Action Sets Details

The Action Sets page provides the following information for each Action configured on the device:

Table 3–7: Action Sets Details

Column	Description
Action Set	The name of the action set
Action(s)	The settings for the actions included in the action set

Table 3–7: Action Sets Details (Continued)

Column	Description
TCP Reset	Indicates whether the option to reset a TCP connection is enabled. With TCP reset enabled, the device can reset the TCP connection for the source or destination IP when the Block action executes. This option can be configured on Block action sets.
Quarantine	Indicates whether the option to Quarantine an IP address is enabled.
Packet Trace	Whether or not packet tracing is enabled
Contact(s)	Where notifications will be sent if a Notification Contact is configured on the action set.
Function(s)  	<p>The functions available to manage the Action Set:</p> <ul style="list-style-type: none"> • Delete a custom action set. You cannot delete a default Action Set or an Action Set that is currently assigned to a filter. • Edit the Action Set configuration. (You cannot edit the <i>Recommended</i> Action Set)

Configure an Action Set

- STEP 1** From the LSM menu, select **IPS > Action Sets**. The IPS Profile - Actions Sets page displays.
- STEP 2** On the Action Sets page, click the **Create Action Set** button, or click the **pencil** for the Action Set you want to edit.
- STEP 3** On the Create/Edit Action Set page, type or edit the **Action Set Name**.
- STEP 4** For **Actions**, select a flow control action setting:
- **Permit** — Allows traffic
 - **Rate Limit** — Limits the speed of traffic. Select a **Rate**.
 - **Block** — Does not permit traffic
- TCP Reset** — Used with the **Block** action, resets the source, destination, or both IPs of an attack. This option resets blocked TCP flows.
- Quarantine** — Used with the Block action, blocks an IP (source or destination) that triggers the filter. See [“Configure a Quarantine Action Set” on page 51](#).
- STEP 5** Optionally, click the **Packet Trace** check box:
- STEP A** Select the **Priority** from the drop-down list: **High**, **Medium**, or **Low**.
- STEP B** Select the **Verbosity** from the drop-down list.
- If you choose partial verbosity, choose how many bytes of the packet to capture (between 64-1600).

STEP 6 Choose one or more **Contacts** by checking the box next to the appropriate **Contact Name**. If there are no contacts displayed, you must [Create an Email or SNMP Notification Contact](#) first.



Note If using Quarantine on a managing SMS, you must add the SMS notification contact to the action sets for filters. Only filters with the SMS contact enabled on actions sets are accessible through the SMS for quarantine.

STEP 7 Click **Create**.

Rate Limit Action Set

A Rate Limit action set defines a maximum bandwidth that can be used by traffic that matches filters assigned to that action set. Incoming traffic in excess of this bandwidth is dropped. If two or more filters use the same rate limiting action set, then all packets matching these filters share the bandwidth. For example, if filters 164 (ICMP Echo Request) and 161 (ICMP Redirect Undefined Code) use the same 10 Mbps action set, then both “Echo Requests” and “Redirect Undefined Codes” filters share the 10 Mbps “pipe” as opposed to each filter getting a dedicated 10Mbps pipe.

The supported rates are subject to restrictions based on the device model. Any of these listed rates can be used as long as it does not exceed 25% percent of the total bandwidth of the product.

The following table lists supported rates.

Device	Supported Rates
X5	50, 100, 150, 200, 300, 400, 500, 600, 700, and 900 Kbps
X506	50, 100, 150, 200, 250, 300, 350, 400, 450, 500, 600, 700, 800, 900 and 1000 Kbps 1.5, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 20, 25, 30, 35, 40, 50, 62, and 83 Mbps

Quarantine Action Set

Quarantine Action Sets are Block action sets configured to block or redirect traffic from the host IP address for the filtered traffic. By enabling quarantine with a Block action set, you reduce the exposure of your network to internal and external threats.

When a filter with a quarantine option triggers, the device installs two blocks: one for the flow (as is normally done with Block actions) and another for the quarantined IP address. In addition to installing the two blocks, the device quarantines the IP address based on the instructions in the action set. For example, the user can display a Quarantine web page to notify the user of the problem and optionally provide instructions for fixing it, or the action may redirect all traffic from the quarantined IP address to a quarantine server that provides instructions to correct the problem.

You can review the list of currently quarantined IP addresses from the Quarantined Streams page (**Events > Managed Streams > Quarantined Streams**). You can also force an address into quarantine, or release a quarantined address. For additional information, see [“Quarantined Addresses” on page 113](#).

For additional information on configuring Quarantine Action Sets, see the following topics:

- [“Quarantine Action Set Configuration Parameters” on page 50](#)
- [“Configure a Quarantine Action Set” on page 51](#)

Quarantine Action Set Configuration Parameters

The following table describes the Quarantine Action Set configuration parameters:

Table 3–8: Quarantine Action Set Configuration Parameters

Parameter	Description
Web Requests	<p>Select an option to specify how the Quarantine action manages HTTP traffic:</p> <ul style="list-style-type: none"> • Block the requests entirely • Redirect the client to another web server • Display quarantine web page with information on the triggered filter and any customized message specified. For details, see “Configure a Quarantine Action Set” on page 51.
Other Traffic	Determines how the device handles other non-HTTP traffic when the Action set is triggered: Block or Permit .
Limit quarantine to the following IP address(es)	Create a list of “limit to” IP addresses. This option limits the filter using this action set to quarantine only those connections and systems matching the IP addresses listed.
Thresholds	<p>Specifies a threshold to prevent network users from being quarantined the first time their network traffic triggers a filter configured with a quarantine action set:</p> <ul style="list-style-type: none"> • Quarantine Threshold is the number of hits before the threshold triggers • Quarantine Threshold Period is the time interval for the hit count <p>For example, if you enter 5 for the Quarantine Threshold and 30 for the Quarantine Threshold Period, only hosts which match a filter 5 times in 30 minutes are quarantined.</p> <p>Threshold parameter limits are 1 to 10,000 hits during a period from 1 to 60 minutes.</p> <p>If Thresholds are not configured, a host is quarantined the first time its traffic matches a filter configured with a quarantine action set.</p>
Do not quarantine the following IP addresses	Create a list of <i>excluded</i> IP addresses which will not be quarantined. Even if a filter with quarantine triggers, these IP addresses will not be quarantined, continuing with other commands in the action set. For example, the action set may include quarantine commands to block the traffic and redirect web requests to a particular server.

Table 3–8: Quarantine Action Set Configuration Parameters (Continued)

Parameter	Description
Allow Quarantined Host Access	Configure a list of IP addresses that a quarantined host is still allowed to access if traffic from the host triggers the Quarantine Action Set.

Configure a Quarantine Action Set

- STEP 1** From the LSM menu, click **Action Sets**.
- STEP 2** On the Action Sets page, click **Create Action Set**, or click the pencil icon for a filter you want to edit.
- STEP 3** On the Create/Edit Action Sets page, type or edit the **Action Set Name**, as needed.
- STEP 4** On the Create/Edit Action Sets page in the **Actions** table, select **Block**. Then, select the **Quarantine** check box.
- The page updates to display the Quarantine Options table.
- STEP 5** Select one of the following options to configure **Web Requests**:
- Select **Block** to block web requests entirely.
 - Select **Redirect to a web server**. Then, type a web server address.
Any received web requests will redirect the client to this web server.
 - Select **Display quarantine web page** to display a quarantined web page. Then, check the types of information to include on the quarantine page. Optionally, enter custom text to display additional information.
- STEP 6** To determine how the device manages quarantine when non-HTTP traffic matches a filter, choose an action: **Block** or **Permit**.
- STEP 7** To limit the quarantine actions to a specific IP addresses, do the following:
- STEP A** In the **Limit quarantine to the following IP address(es)** table, enter a **Source Address**.
- STEP B** Click **add to table below**.
- STEP C** Repeat to add multiple IP addresses.
- STEP 8** Configure **Threshold** settings to specify the number of filter matches are required before the quarantine action is executed.
- STEP 9** To perform the quarantine actions without affecting specific IP addresses, do the following:
- STEP A** In the **Do not quarantine the following IP address(es)** table, enter a **Source Address**.
- STEP B** Click **add to table below**.
- STEP C** Repeat to add multiple IP addresses.
- STEP 10** To allow quarantined clients access to hosts:

STEP A In the **Allow quarantined hosts to access the following IP address(es)** table, enter a **Destination Address**.

STEP B Click **add to table below**.

STEP C Repeat to add multiple hosts.

STEP 11 Click **Create/Save**.

Notification Contacts

Configuring notification contacts allows you to send messages to a recipient (either human or machine) in response to a traffic-related event that occurs on the X family device. The traffic-related event can be the result of triggering an IPS filter configured with an action set that specifies a notification contact, or by triggering a Firewall Block rule with syslog logging enabled. A notification contact can be any of the following:

- **Remote System Log** — Sends messages to a syslog server on your network. This is a default contact available in all IPS action sets. Before using this contact, configure the IP address and port for the syslog server (**System > Configuration > Syslog Servers**). The Remote System Log is also the destination for all messages from Firewall Block rules with the **enable syslog logging option** turned on.
- **Management Console** — Sends messages to the LSM or the SMS device management application. This default contact is available in all action sets. If this contact is selected messages are sent to the Alert or IPS Block Log in the LSM, depending on whether a permit or block action has executed. When the device is under SMS management, messages are also sent to the SMS client application. This notification contact does not require any configuration, although you can change the default name and aggregation period.
- **Email or SNMP** — Sends messages to the email address or specified SNMP. All email or SNMP contacts must be added from the Notification Contacts page. If the default email server is not configured on the device, you will be prompted to configure it before adding a contact.

After configuring notification contacts, you can select them for IPS filter events when you create or edit the action set assigned to the filter. For Firewall Block rules, you can specify that messages be sent to the Remote System Log contact by selecting the **enable syslog logging** option when you edit the rule.

Alert Aggregation and the Aggregation Period

The X family uses Alert Aggregation to protect system performance. Because a single packet can trigger an alert, attacks with large numbers of packets could potentially flood the alert mechanism used to send out notifications. Alert aggregation allows you to receive alert notifications at intervals to prevent this flooding. For example, if the aggregation interval is 5 minutes, the device sends an alert at the first IPS filter trigger, collects subsequent alerts and sends them out every five minutes.

On the device, alert aggregation is controlled by the *aggregation period* that you configure when you create a notification contact. This setting is required for all notification contacts. For Email contacts, the aggregation period works in conjunction with the *Email Threshold* setting configured for the Email Server. By default, the device allows ten (10) email alerts per minute. On the first email alert, a one

minute timer starts. The device sends e-mail notifications until the threshold is reached. Any notifications received after the threshold is reached are blocked. After one minute, the device resumes sending email alerts. The device generates a message in the system log whenever email notifications are blocked.



CAUTION Short aggregation periods can significantly affect system performance. The shorter the aggregation period, the higher the system load. In the event of a flood attack, a short aggregation period can lead to system performance problems.

In addition to the user-configured aggregation period, the device also provides alert aggregation services to protect the device from over-active filters that can lower performance.

For details on configuring Notification Contacts, see the following topics:

- [“Create an Email or SNMP Notification Contact” on page 53](#)
- [“Configure the Remote System Log Contact” on page 54](#)
- [“Configure the Management Console Contact” on page 54](#)
- [“Delete a Notification Contact” on page 54](#)

Create an Email or SNMP Notification Contact



Note Before creating an Email or notification contact, you must to configure Email and SMTP server settings on the device from the Email Server page (**System > Configuration > Email Server**). For details, see [“Email Server” on page 241](#).

- STEP 1** From the LSM menu, select **IPS > Action Sets**. Then, choose the **Notification Contacts** tab.
- STEP 2** On the Notification Contacts page, click the **Add Contact** button or select the **pencil** icon for the contact you want to edit.
- STEP 3** Type **Contact's Name**. This name is used to manage the contact information on the Notification Contacts page.
- STEP 4** Enter the address where notifications will be sent in the **To Email Address** field.
- STEP 5** Enter the **Aggregation Period**.
Longer aggregation periods improve system performance.
- STEP 6** Click **Create** to save the changes.
- STEP 7** Optionally, click the **Test Email** button.

If you click the button, the IPS attempts to send an email message, using the server defined in the default email settings, to the email contact you are creating.

If the email fails to send properly, check for the following possible causes:

- Is default email server configured? See [“Email Server” on page 241](#).
- Email server must be reachable from the device. In the CLI use the PING command to see if you can reach email server IP.
- Email server may not allow mail relaying. Make sure you use account/domain that the email server accepts.

Configure the Remote System Log Contact



CAUTION Remote syslog, in adherence to RFC 3164, sends clear text log messages using the UDP protocol with no additional security protections. Therefore, you should only use remote syslog on a secure, trusted network to prevent syslog messages from being intercepted, altered, or spoofed by a third party.

- STEP 1** From the LSM menu, select **IPS > Action Sets**. Then, on the Action Sets page, click the **Notification Contacts** tab.
- STEP 2** On the Notification Contacts page in the **Contacts List**, click the **Remote System Log** link.
- STEP 3** On the Edit Notification Contact page, type the **IP Address** and **Port** for the host that receives the offloaded log messages.
- STEP 4** Type the **IP Address** and **Port** for the host that will receive Remote System Log messages.



TIP Verify that the device can reach the remote system log server on your network. If the remote system log server is on a different subnet than the device management port you may have to add static routes (see [“Static Routes” on page 159](#)).

- STEP 5** Select an **Alert Facility** and a **Block Facility**: none or select from a range of 0 to 31. These syslog number uses these numbers to identify the message source.
- STEP 6** Select a **Delimiter** for the generated logs: **tab**, **comma**, **semicolon**, or **bar**.
- STEP 7** Click **Add to table below** to add the remote syslog server.
- STEP 8** Enter a **Remote system log aggregation period** in minutes.
- STEP 9** Click **Save**.

Configure the Management Console Contact

- STEP 1** From the LSM menu, select **IPS > Notification Contacts**. Then, click the **Notification Contacts** tab.
- STEP 2** Click the **pencil** icon next to the Management Console entry.
- STEP 3** Edit the **Contact Name**. By default, it is Management Console.
- STEP 4** Enter the **Aggregation Period** for notification messages in minutes.
- STEP 5** Click **Save**.

Delete a Notification Contact



Note You cannot delete the default Remote System Log and Management Console contacts

- STEP 1** From the LSM menu, select **IPS > Action Sets**. Then, click the **Notification Contacts** tab.
- STEP 2** On the Notification Contacts page, click the **Delete** icon to remove the notification contact.

You cannot delete a Notification Contact if it is currently configured on an Action Set.

STEP 3 On the confirmation dialog, click **OK**.

IPS Services

Use the Services page (**IPS > Services**) to add and manage non-standard ports supported by the device. This feature enables you to configure additional ports associated with specific applications, services, and protocols to expand scanning of traffic. First filters scan traffic against the standard ports for listed services, the engine then accesses and scans traffic against the list of additional ports. Each service supports up to 16 additional ports.

The following figure shows the IPS Profile - Services page:

Figure 3–8: IPS PROFILE - Services Page

Application	Protocol	User-Defined Ports	System-Defined Ports
pop3	tcp		110
rsh	tcp		514
auth	tcp		113
snmp	udp		161
imap	tcp		143
portmapper	tcp		111 32770 32771 32772 32773 32774 32775 32776 32777 32778 32779
ircu	tcp		6665 6666 6667 6668 6669 7000
smb	tcp		139 445
dns	tcp		53
ssh	tcp		22
ms-sql	tcp		1433
ftp	tcp		21
portmapper	udp		111 32770 32771 32772 32773 32774 32775 32776 32777 32778 32779
smtp	tcp		25
dns	udp		53
telnet	tcp		23
http	tcp		80 3128 8000 8080
pop2	tcp		109
nntp	tcp		119
rlogin	tcp		513
snmp	tcp		161
finger	tcp		79

From the IPS Services page, you can complete the following tasks:

- Add an additional port configuration
- Delete a custom port configuration

For additional information, see the following topics:

- [“IPS Services Page Details” on page 56](#)
- [“Add a Port” on page 56](#)
- [“Delete a Port” on page 56](#)

IPS Services Page Details

The IPS Services page provides the following information:

Table 3–9: IPS: IPS Services Details

Parameter	Definition
Application	Type of application/network service
Protocol	The protocol for the application
User-Defined Ports	The list of the custom ports defined on the X family. Ports are listed in order with a space between each number.
System-Defined Ports	The list of supported ports per application. Ports are listed in order with a space between each number.

Add a Port

- STEP 1** From the LSM menu, click **IPS Services**.
- STEP 2** On the IPS Services page, click **Add Port Configuration**.
- STEP 3** On the Create Port Configuration page in the Application Type/Port Assignment table, select the **Application Type**. Then, enter a **Port Number**.
- STEP 4** Click **Create**. Then, click **OK** on the confirmation pop-up.

Delete a Port



Note You cannot delete any of the default port configurations configured on the X family device.

- STEP 1** From the LSM menu, click **IPS Services**.
- STEP 2** On the IPS Services page, click **Delete Port**.
- STEP 3** On the Delete Port Configuration page, select the **Application Type** for the port configuration to delete.
- The selection list only includes applications that have been configured with a custom port.
- STEP 4** Select a **Port Number** to delete.
- You can only delete one port at a time.
- STEP 5** Click **Delete** to delete the port and return to the IPS Services page.

Preferences

Use the IPS Preferences page (**IPS > Preferences**) to configure settings related to the Threat Suppression Engine and filtering performance. From this page you can complete the following tasks:

- Reset all filters to the factory default settings
- Configure timeouts, logging, and other settings for the Threat Suppression Engine
- Change the global settings for the Adaptive Filter function
- View the most recent filters affected by the Adaptive Filter configuration

The following figure shows the IPS Preferences pane.

Figure 3–9: IPS Preferences

IPS Preferences

Reset Filters

Reset Filters Clicking "Reset Filters" will reset your filter configuration to its factory default values.

Configure Threat Suppression Engine (TSE)

Connection Table Timeout: 1800 seconds (30-1800 seconds)

☒ Automatically release addresses from quarantine after specified duration

Quarantine Timeout: 60 minutes (1-1440 minutes)

Logging Mode: ☐ Always ☒ Disable if congested

Congestion Percentage: 1.0 % (0.1 to 99.9)

Disable Time: 600 seconds (60 to 3600)

If the mode is "Disable if congested", logging will be disabled for the specified amount of time when the congestion percent is reached. Otherwise logging will always occur.

Adaptive Configuration Settings

Mode: ☒ Auto ☐ Manual

Log Severity: Warn

Ten Most Recent

Filter Name	Filter State	Adaptive Config State	Function(s)
No Entries			

Reset Filters

To restore IPS filters and associated settings to the factory default settings, use the Reset Filters option available on the Preferences page.



CAUTION The Reset Filter action restores all filters back to their recommended Category Settings. You will lose any filter customizations made in the Security Profiles. You will also lose any user-created Action sets, rate limits, and traffic thresholds, etc. You cannot undo this action.

Reset the IPS Filters to Factory Default Settings

STEP 1 From the LSM menu, select **IPS > Preferences**.

STEP 2 On the IPS Preferences page, click **Reset Filters**. Then, click **OK** on the confirmation pop-up.

Configure Threat Suppression Engine (TSE)

On the IPS Preferences page, configure global settings for the TSE in the Configure Threat Suppression Engine table. Refer to the following table for a description of the TSE configuration parameters:

Table 3–10: IPS Preferences: TSE Configuration Parameters

Parameter	Description
Connection Table Timeout	<p>Specifies the global timeout interval for the connection table. For blocked streams in the connection table, this value determines the time interval that elapses before the blocked connection is cleared from the connection table. Before the timeout occurs, any incoming packets for that stream are blocked at the device. After the connection is cleared (the timeout interval expires), the incoming connection is allowed until or unless traffic matches another blocking filter.</p> <p>Note Blocked streams can also be cleared from the connection table manually from the Blocked Streams page (Events > Managed Streams > Blocked Streams).</p>
Quarantine Timeout	<p>The value for the quarantine timeout. This value applies to all quarantined addresses and determines the amount of time that elapses before the address is released from quarantine.</p> <p>Note Quarantined streams can also be released manually from the Quarantined Streams page (Events > Managed Streams > Quarantined Streams).</p>
Logging Mode	<p>Configure settings to prevent traffic-related event notifications (such as those generated when a triggered filter is configured with a <i>Block+Notify</i> or <i>Permit+ Notify</i> action set) from causing network congestion.</p> <ul style="list-style-type: none"> • Logging Mode determines whether logging is enabled/disabled when the network becomes congested. Always indicates that the device continues logging even if traffic is dropped under high load. Disable if congested indicates the logging will be disabled when the device reaches the specified congestion percentage. • Congestion Percentage can be configured if the disable logging option is selected. This value specifies the amount of network congestion that can occur before the device disables logging functions. • Disable Time specifies the amount of time (default is 10 minutes) that logging is disabled before the service is restarted. When the downtime expires, the device re-enables logging and displays the number of missed notifications.

Configure Global Settings for the TSE

- STEP 1** From the LSM menu, select **IPS > Preferences**.
- STEP 2** On the IPS Preferences page in the **Configure Threat Suppression Engine (TSE) table**, change the configuration parameters as required.
- To configure the Quarantine Timeout, check **Automatically release addresses from quarantine after specified duration**.
- To configure **Congestion Percentage** and **Disable Time** for the disable logging feature, select **Disabled if congested in** the **Logging Mode** field.
- STEP 3** Click **Apply**.

Adaptive Filter Configuration

You can configure the global settings for the Adaptive Filter from the IPS Preferences page (**IPS > IPS Preferences**) and the Configure Adaptive Filter Events page (**Events > Reports > Adaptive Filter**). At the filter level, you have the option to disable Adaptive Filter configuration so that a filter is never impacted by Adaptive Filter settings on the device. For details, see [“Edit DV Filter Category Settings” on page 29](#).

For additional information, see the following topics:

- [“How Adaptive Filtering Works” on page 60](#)
- [“Restrictions” on page 60](#)
- [“Tuning Adaptive Filter Configuration” on page 60](#)

How Adaptive Filtering Works

Adaptive Filtering is a mechanism to configure the Threat Suppression engine to automatically manage filter behavior when the X family device is under extreme load conditions. This feature protects your network against the potential adverse affects of a filter that interacts poorly with the network environment by preventing the device from entering High Availability mode.

Adaptive filtering works by monitoring each filter to identify any suspected of causing congestion. When it identifies a filter, it manages the filter using one of the following methods, depending on how the global or filter-level Adaptive Filtering is configured:

- **Automatic Mode** — This setting enables the device to automatically disable and generate a system message regarding the problematic filter.
- **Manual** — This setting enables the device to generate a system message regarding the problematic filter. However, the filter is not disabled.

Restrictions

You cannot configure adaptive filter settings for Traffic Threshold, Reconnaissance, or Traffic Normalization filters.

Tuning Adaptive Filter Configuration

You can view the ten filters most recently affected by the Adaptive Filter Configuration in the **Ten Most Recent** table available on the IPS Preferences page and the Configure Adaptive Filter Events page (**Events > Reports > Adaptive Filter**). From this table, you can click on a filter name to change the global or filter-level AFC settings. For details on this table, see [Table 5–16, “TSE Adaptive Filter Configuration Details,” on page 126](#). You can manage global AFC configuration by modifying the Mode and Log Severity settings on either the IPS Preferences page or the Configure Adaptive Filter Events page.

Configure the global TSE Adaptive Filter Setting

- STEP 1** From the LSM menu, select **IPS > Preferences**.
- STEP 2** On the IPS Preferences page in the **Adaptive Configuration Settings** table, select the mode:
- **Automatic Mode** — This setting enables the X family device to automatically disable and log any defective filter.
 - **Manual** — This setting enables the device to log any defective filter without disabling it.

- STEP 3** Select the **Log Severity** of the system log message that is automatically generated when a filter triggers the Adaptive Filter function.
- STEP 4** Click **Apply**.

4 Firewall

The Firewall section describes how to enable, disable, and modify firewall rules and various features using the Firewall Rules table. This section also details virtual servers, services, service groups, and schedules.

Overview

The X family provides a Stateful Packet Inspection Firewall, providing session level control for IP-based protocols. The firewall can perform advanced session-oriented functionality including Network Address Translation (NAT), Web Filtering, Virtual Servers (DMZ), and traffic prioritization.

The firewall only opens TCP or UDP ports between two IP addresses when the firewall rules permit the communication. Secondary connections (for protocols such as FTP and SIP) are opened automatically where appropriate, and only for the duration of the primary session.

Firewall rules control the flow of traffic between Security Zones, provide bandwidth management, and ensure quality of service. You can use firewall rules to:

- Determine when and how traffic will be classified and controlled by the X family device.
- For local users that have been authenticated, determine whether the user has permission to access the requested service, based on the privilege group the user belongs to.
- Prioritize specific types of network traffic.
- Allow or deny a session request.
- Apply web filtering to specific categories.
- Schedule when a service will be denied or allowed.
- Allocate bandwidth resources to a service and ensure a service has available bandwidth.
- Limit bandwidth resources to certain services.
- Time out idle sessions.
- Monitor network traffic.

For a full description of firewall rules, together with configuration examples, refer to the *Concepts Guide*.

You can view and manage Firewall Rules and configuration options from the Firewall menu pages. The menu provides the following options:

- **Firewall Rules** — Allows you to manage and configure security policy to monitor traffic between security zones. You can also specify IP hosts/subnets/ranges to monitor traffic within a specified zone. You can optionally configure services, rate limiting, scheduling, authentication, and web filtering as part of each firewall rule.
- **Services** — Manage services based on applications and protocols that can be configured in a firewall rule to police the traffic. The X family device supports a predefined list of services and also allows you to define custom services and IP protocol numbers. You can also create a **Service Group** so you can configure one firewall rule to apply to multiple services without having to configure each service separately. You only need to configure services if you want to change the port and protocol settings for an existing service, or create a new service.
- **Schedules** — The X family device allows you to create schedules, which are used to limit when a firewall rule operates. Schedules contain intervals of days and hours when the firewall rule applies. You only need to configure schedules if you require a firewall rule that will only apply at certain days and times.
- **Virtual Servers** — The X family device allows you to configure virtual servers on your LAN, which are protected by the device firewall, so they can be accessed from the Internet or another security zone without exposing the internal network IP addresses. You should configure virtual servers for internal servers that need to be reached from the internet. A common application for Virtual Servers is to create a Demilitarized Zone (DMZ).
- **Web Filtering** — Web filtering allows you to configure a subscription-based content filtering service and/or specify URL filters to permit or deny traffic based on specific URLs or URL patterns. To enable web filtering, you must configure a firewall rule with the action set to *Web Filtering*.



Note Before setting up Firewall Rules, verify that the Network configuration (IP address groups, Virtual Interfaces, and Security Zones) has been set up correctly for your environment. For information, see [Chapter 6, “Network”](#).

For details, see the following sections:

- [“How Firewall Rule Enforcement Works” on page 64](#)
- [“Default Firewall Rules” on page 67](#)
- [“Managing Firewall Rules” on page 68](#)
- [“Firewall Services” on page 75](#)
- [“Schedules” on page 79](#)
- [“Virtual Servers” on page 82](#)

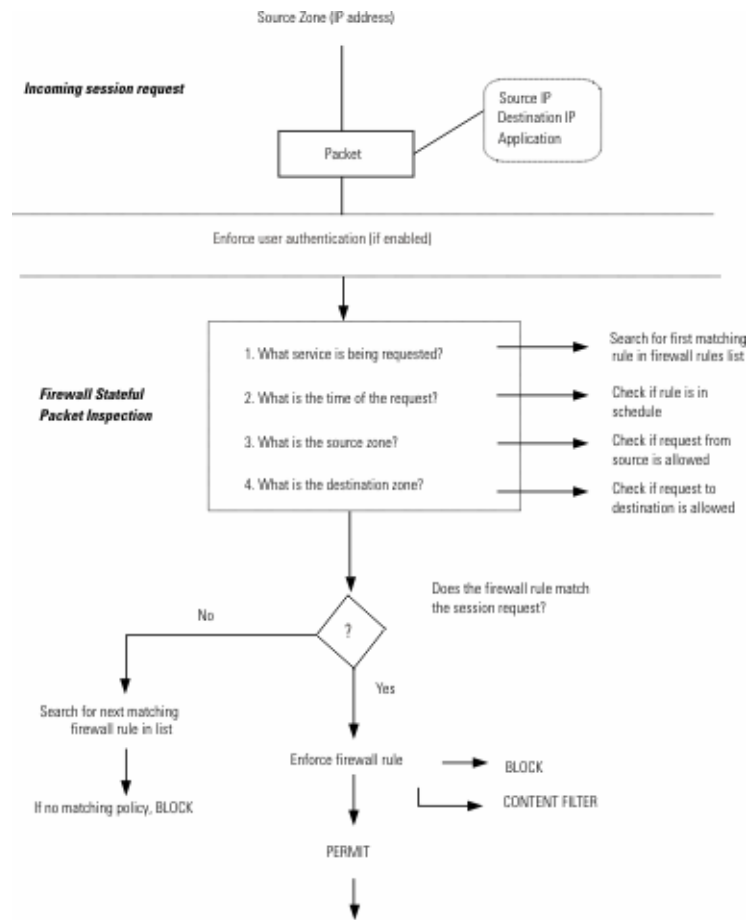
How Firewall Rule Enforcement Works

The following is an example of how the X family enforces firewall rules for a session request, for example, when a user requests a Web page using a browser.

- STEP 1** The user starts a web browser. The web browser resolves the DNS name for the URL and initiate a TCP connection to the target web server via the X family device.
- STEP 2** The X family device inspects the session header and identifies the following information about the request:
- Source IP — The address of the device that initiated the request.
 - Destination IP — The address of the device for which the request is intended.
 - Application — Type of service/content and authenticated user (if any).
- STEP A** Using its routing table, the device decides which Security Zone the session has come from and which zone it is going to.
- STEP 3** The device searches for the first firewall rule in its list that matches the session request. Rules are evaluated based on what options are configured:
- user authentication
 - IP protocol service
 - schedule
 - source zone
 - destination zone
 - web filtering

The firewall rule table is searched from the top of the table to the end (if necessary) looking for the first firewall rule that will match the session. Thus, it is important to put the most specific rules (for example, those configured with user authentication, IP address groups/ranges, or web filtering) towards the top of the table. The following diagram illustrates how session requests are evaluated.

Figure 4–1: Handling Firewall Session Requests



- STEP 4** When a rule is matched, the device enforces the firewall rule based on the action and logging configuration for the rule: Traffic is either permitted or blocked; the event is entered in the local log, sent to a remote syslog server, or not logged at all.
- STEP 5** If no matching firewall rule is found in the firewall rules list, the device denies the request using the implicit deny rule preconfigured on the device. For details, see [“Default Firewall Rules” on page 67](#).

For additional information on setting up firewall rules, see the following topics:

- [“Default Firewall Rules” on page 67](#)
- [“Managing Firewall Rules” on page 68](#)
- [“Firewall Services” on page 75](#)
- [“Schedules” on page 79](#)
- [“Virtual Servers” on page 82](#)

Default Firewall Rules

The following table lists the default firewall rules available on the X family device. You can add, delete or edit these rules. However, be careful when editing or deleting the default rules as this may prevent you from configuring the device or accessing some services on the device. If this does happen, you can restore access by resetting the device to factory default settings using the instructions provided in the *Hardware and Installation Guide*.

Table 4–1: Default Firewall Rule Configuration

ID	Action	Source Zone	Dest Zone	Service	Logging	State	Description
1	Permit	LAN	WAN	ANY	Off	Enabled	Allow LAN unrestricted access to WAN
2	Permit	ANY	this-device	vpn-protocols	Off	Enabled	Allow VPN termination
3	Permit	LAN	this-device	management	Off	Enabled	Allow management access from LAN via https, ssh, snmp, or ping
4	Permit	LAN	this-device	network protocols	Off	Enabled	Allow DNS and DHCP-server from LAN

Table 4–1: Default Firewall Rule Configuration (Continued)

ID	Action	Source Zone	Dest Zone	Service	Logging	State	Description
	Permit	this-device	ANY	ANY		Enabled	This is an implicit firewall rule that cannot be modified or viewed from the LSM. It is needed for AutoDV, Web Filtering, and other features. This rule also allows the Network Tools to operate.
	Block	ANY	ANY	ANY		Enabled	Implicit rule that blocks all other traffic with a silent drop.

The default firewall rules configured for the *this-device* zone use the LAN security zone. The management IP address of the X family device is any of the IP interface addresses. The device IP address is not generally accessible to the LAN by ping (or other services) unless a firewall rule allows such access. The device allows you to configure a firewall rule to prevent access to the management interface, even from the LAN security zone.



Note If you delete the **this-device** zone, you may only be able to access the device using the command line interface (CLI) on the serial port.

For a detailed explanation of firewall rule concepts together with an example firewall implementation, see the *Concepts Guide*.

For additional information on managing firewall rules from the LSM, see the following topics:

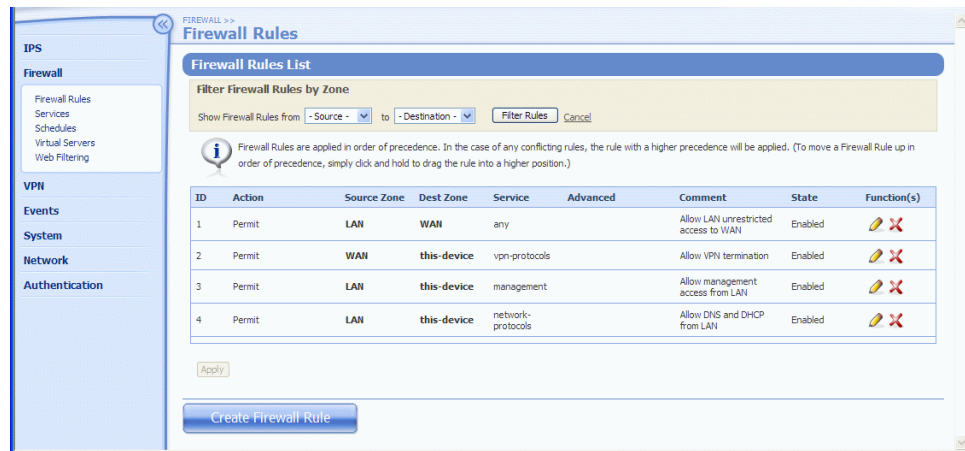
- [“Managing Firewall Rules” on page 68](#)
- [“Configuring Firewall Rules” on page 71](#)

Managing Firewall Rules

The Firewall Rules page (**Firewall > Firewall Rules**) displays a list the firewall rules currently configured on your X family device. From this page, you can view, edit, enable, disable, and re-order firewall rules.

The following figure shows the Firewall Rules page.

Figure 4–2: FIREWALL - Firewall Rules Page



You can complete the following tasks from the Firewall Rules page:

- Create/Edit a firewall rule
- Delete a firewall rule
- Filter the Firewall Rules List to display only those configured for a user-specified Source and Destination zone.

When the **Firewall Rules List** is filtered, the LSM only shows filters that match the criteria selected in the **Filter Firewall Rules by Zone** filter options.








Firewall Rules List Details

The Firewall Rules List page displays the following information for each rule in the list:

Table 4–2: Firewall Rules List Details

Column	Description
ID	A unique ID system-assigned to the firewall rule.
Action	The action that will be applied when this firewall rule is matched for a given session. Either Permit or Block or Web Filter.
Source Zone (Addresses)	Indicates the Source Security Zone for the session request. By default, the source zone includes all IP addresses within the given zone. If the firewall rule has been configured to apply only to a subset of IP addresses, the subset (IP address group, subnet, IP address range) is displayed.
Destination Zone (Addresses)	This field indicates the destination security zone where traffic will be directed if it is permitted. By default, the destination zone includes all IP addresses within the given zone. If the firewall rule has been configured to send permitted traffic to only a subset of IP addresses, the subset (IP address group, subnet, IP address range) is displayed.

Table 4–2: Firewall Rules List Details (Continued)

Column	Description
Service	The service or service group associated with the firewall rule. The firewall rule only applies to a session request for the specified service or service within the specified Service Group. If ANY is specified, the firewall rule applies to all services available.
Advanced	<p>The icons indicate which advanced options are enabled for the firewall rule. If a feature is enabled, an icon representing the feature is displayed in the Firewall Rules List page. Available options are:</p> <ul style="list-style-type: none">  • Bandwidth Management (traffic shaping) — If this option is configured, any traffic permitted by the firewall rule is given the bandwidth priority and rate specified in the firewall rule.  • Schedule — If this option is configured, the firewall rule is only applied during the days and times configured in the firewall rule schedule.  • User Authentication — If this option is configured, the firewall rule is only applied to local users who have been authenticated by the device. For details on user authentication, see the “How Local User Authentication Works: RADIUS, Privilege Groups and X.509 Certificates” on page 251.  • Logging Enabled — If this option is configured, any event triggered by the firewall rule (Permit or Block) is entered into the appropriate log.
Comment	The firewall rule description entered when the rule was created.
State	Whether the firewall rule is enabled (checked) or disabled (not checked)
Functions	<p>Icon representing functions available to manage the firewall rule. The following functions are available.</p> <ul style="list-style-type: none">  • Edit the firewall rule.  • Delete the firewall rule.  • Add firewall rule — clicking this icon in a firewall rule entry allows you to create a firewall rule that will be added above the rule selected.

For additional information, see the following topics:

- [“Firewall Rules List Details” on page 69](#)
- [“Configuring Firewall Rules” on page 71](#)
- [“Create/Edit a Firewall Rule” on page 72](#)
- [“Change the Order in which Firewall Rules are Applied” on page 75](#)

Configuring Firewall Rules

When configuring a firewall rule, you must define the action, logging options and other components that make up the rule. Before you can configure the firewall rule, the components should be configured so that they are available for selection during the configuration process. The following describes the firewall rule components:

- **Action** — This is a required component that determines how the X family device manages packets when the firewall rule is matched. You can configure the firewall to *Permit*, *Block*, or perform web filtering on traffic that matches the firewall rule.
- **Services** — When you configure a firewall rule, you must select the service or service group to which it will be applied. The device provides predefined services which are applications known to the device such as HTTP, HTTPS, and DNS. You can also configure custom services to manage any IP protocol. For details on configuring services and service groups, see [“Firewall Services” on page 75](#).
- **Source and Destination Address** — All firewall rules must specify the source and destination addresses of the devices to which the firewall rule applies. This is specified using Security Zones. If necessary, you can limit the rule to apply to certain IP addresses within a security zone. For details on setting up Security Zones, see [“Security Zone Configuration” on page 135](#).
- **IP Addresses** — To limit the firewall rule to apply only to certain devices within a Security Zone, you can specify an IP address group, IP Subnet, or IP address range. For IP Address Group configuration details, see [“IP Address Groups” on page 153](#). The default IP address setting for the source and destination zones is to apply the firewall rule to all IP addresses within the zone.
- **Schedules** — Optionally, you can configure the firewall rule to only be applied during certain days and times using the Schedule component. For details on configuring schedules, see [“Schedules” on page 79](#).
- **Logging Options** — Determines whether the X family device creates a log entry when the firewall rule is triggered. For example, if local logging is enabled on a firewall that blocks traffic, the device generates an entry in the Firewall Block log. If remote logging is enabled, the device generates an entry and sends it to the Remote Syslog server or Syslog Server configured on the device. If logging is enabled on a firewall permit rule, the device generates a session start and session end log entry in the Firewall Session Log. For details on the syslog servers, see [“Configuring Remote System Logs” on page 105](#). When you create a firewall rule, logging is disabled by default.

Advanced Options

When creating or editing a firewall rule, you can configure advanced options to enable Bandwidth Management and User Authentication for the firewall rule:

- **Bandwidth Management** — If this option is selected, you can define the guaranteed and maximum bandwidth available for your sessions, to apply the guaranteed bandwidth on a per session or per rule basis, and to prioritize the bandwidth for a session.
- **User Authentication** — If this option is selected, the rule will only be applied if the rule otherwise matches the selection (correct service and IP address, for example), and a local user with appropriate matching privileges has previously authenticated with the X family device. This authentication may be the result of logging in via the SSH or HTTPS interfaces, or by using a VPN client terminating on

the device. If a local user has not been authenticated, the rule is ignored and lower priority rules are examined to find a match the session.



Note For additional information on the advanced options, refer to the **Concepts Guide**.

Configuration Notes

- When a firewall rule is created, the default settings are to enable the firewall rule, disable local and remote logging, and position the firewall rule at the end of the firewall rules table.
- After configuring a firewall rule, it will appear in the firewall rules table. You can disable firewall rules so that the device ignores the rule when inspecting traffic. If necessary, you can re-enable the rule at a later date.


Create/Edit a Firewall Rule



Note For firewall configuration examples, refer to the **Concepts Guide**.

STEP 1 From the LSM menu, select **Firewall > Firewall Rules**.

STEP 2 On the Firewall Rules page, click the **Create Firewall Rule** button at the bottom of the page, or click the **Edit** icon for the rule you want to edit. You may have to scroll down to access the button.

To create a firewall rule above another rule in the table, click the  icon for the firewall rule positioned below the rule you want to create.

STEP 3 On the Create/Edit Firewall Rule page in the **Firewall Rule Setup** table, enter the setup information:

STEP A If you want to apply the firewall rule, click **Enable Firewall Rule**.

STEP B Select the **Action** you want the rule to apply to the traffic, either **Permit** or **Block** or **Web filter**.

STEP C From the **Service** drop-down list, select the Service or Service Group that the rule will apply to.



Note To add a new service or service group, select **Firewall > Services** to open the Firewall Services page. Then, define the service. You can then define firewall rules for the service or group.

STEP D From the **Schedule** drop-down list, select the schedule you want the rule to use, if any.
By default, a firewall rule can be applied 24 hours a day, 7 days a week. This is equivalent to having a schedule of 00:00 to 00:00 defined.

STEP E In the **Inactivity Timeout** field, enter the interval (between 1 and 999 minutes) after which you want any established session to be terminated if there is no activity.

STEP F If desired, type a description for the rule in the **Comment** field.

STEP G To record sessions matching this firewall rule in the Firewall Session Log (for permitted sessions) or Firewall Block log (for blocked sessions), check **Enable logging**.

To offload log entries to a remote syslog server, check **Enable syslog** logging.

STEP 4 In the **Network** table, configure the **Source** zone parameters.

STEP A From the **Source Zone** drop-down list, select the source security zone for this firewall rule.

Select **ANY** from the list if you want the firewall rule to match traffic from any source zone.

Select **this-device** from the list if you want to match traffic from the X family device itself, for example to allow the device to send HTTP packets, Auto DV Update requests, or Web Filter requests to the LAN.



Note An implicit this-device ==> ANY rule is provided by default at the end of the firewall rule table. We recommend not overriding this implicit rule.

STEP B For **Source IP**, select the IP addresses in the source zone to which you want to apply the rule, either:

- Select **All IP addresses**. This is the default selection.
- Select **IP Address Group** and then select the group from the drop-down list.
- Select **IP Subnet** and type the IP address/subnet mask.
- Select **IP Range** and type the range of IP addresses.

STEP 5 In the **Network** table, configure the **Destination** zone parameters.

STEP A From the **Destination Zone** drop-down list, select the destination security zone for this firewall rule.

Select **ANY** from the list if you want the firewall rule to match traffic to any destination zone.

Select **this-device** from the list if you want to match traffic destined for the X family device itself, for example to allow you to manage the device using HTTPS, allow Auto DV Updates, or Web Filtering.

STEP B For **Destination IP**, select the IP addresses in the destination zone to which you want to apply the rule; do one of the following:

- Select **All IP addresses**. This is the default setting.
- Select **IP Address Group** and then select the group from the drop-down list.
- Select **IP Subnet** and enter the IP address/subnet mask.
- Select **IP Range** and enter the range of IP addresses.

STEP 6 In the **Firewall Rule Setup (Advanced)** table, if required, check **Enable bandwidth management**. Bandwidth management only works on Permit rules.

To control the rate of traffic flow between zones, configure bandwidth management as follows:

STEP A In the **Type** field, choose the type of bandwidth management to be applied, either:

- Select **Per Rule** to indicate that the total bandwidth will be shared by all sessions that match the rule.
- Select **Per Session** to indicate that the specified amount of bandwidth will be available to every session that matches the rule.

STEP B Enter the **Guaranteed Bandwidth** (between 1 and 1000000 Kbps).

This value mainly provides pre-allocated bandwidth for particular traffic. The X family device ensures that a session that matches this firewall rule is provided with this bandwidth. (In effect, the device throttles other non-prioritized traffic to ensure this.)

STEP C Enter the **Maximum Bandwidth** (between 1 and 1000000 Kbps).

If a session attempts to use more than its maximum bandwidth, the excess packets are dropped.

STEP D Select the **Bandwidth priority** you want to apply to the session from the drop-down list, where 0 is the highest priority and 3 is the lowest priority.

The X family device transmits higher priority session packets before lower priority session packets. Use priority 0 for applications that require low latency, such as Voice over IP.



Note Generally, bandwidth management works best if a small amount of traffic is prioritized as priority 0 over all other traffic via a single bandwidth management rule. A good example is prioritizing voice traffic over everything else. It is not recommended to use priorities 1-3 to form complex bandwidth management policies. Such configurations are hard to define and harder to verify working.

STEP 7 If required, check **Only apply firewall to authenticated users** in the **Firewall Rule Setup (Advanced)** table to turn on authentication for this firewall rule.

- To enable all users that have firewall rule authentication enabled to be authenticated, select **Any privilege group with policy authentication**.
- To limit authentication to members of a particular privilege group, select that privilege group from the drop-down list.

STEP 8 Click **Create** to save the firewall rule.

Click **Cancel** to return to the **Firewall Rules Summary** without saving the changes.

Enable or Disable a Firewall Rule

STEP 1 From the LSM menu, select **Firewall > Firewall Rules**.

STEP 2 On the Firewall Rules page in the **Firewall Rules List** table, click the **Edit** icon for the firewall rule you want to edit.

STEP 3 On the Edit Firewall Rule page in the **Firewall Rule Setup** table, click the **Enable** check box to enable the rule.

To disable the rule, clear the check box.

STEP 4 Click **Save**.

Change the Order in which Firewall Rules are Applied

STEP 1 From the LSM menu, select **Firewall > Firewall Rules**.

STEP 2 On the Firewall Rules page, select the row you want to move. Then, drag the rule to the desired location.

Firewall Services

Firewall Services and Service Groups are used to specify Firewall Rules and Virtual Servers.

- **Firewall Service** — An application or protocol that can be configured in a firewall rule to police traffic. For example, to monitor all traffic from the http service, select the http service when you configure the firewall rule for this policy. You can also specify a specific IP protocol to police. For device maximum configurable values, see [“Appendix D, “Device Maximum Values”](#).
- **Firewall Service Group** — A logical grouping of services that allows you to configure a firewall rule or virtual server to apply to traffic from more than one service. For example, the dns Service Group includes the dns-tcp and dns-udp services. To monitor all dns-tcp and dns-udp traffic, select the dns Service Group when you configure the firewall rule for this policy. You can have up to 50 Service Groups on an X family device.

Service groups allow you to configure a single firewall rule or virtual server to apply to traffic from a collection of services rather than creating individual configurations for each service. After the

Service and Service Groups have been configured, you can assign them to firewall rules or virtual servers based on your network security requirements.

Use the Firewall Services page (**Firewall > Services**) to view and manage Services and Service Groups. The following figure shows the Firewall Services page.

Figure 4–3: Firewall - Firewall Services Page

Firewall Services			Firewall Service Groups	
Service	Protocol	Ports	Service Group	Service(s)
3com-nbx	17	2093 - 2096	dns	dns-tcp, dns-udp
audio-call-control	6	1731	email	pop3, smtp, imap, imapv3
dhcp-client	17	68	ipsec	ike, ipsec-ah, ipsec-esp
dhcp-server	17	67	ldap	ldap-udp, ldap-tcp
dns-tcp	6	53	management	https, ssh, ping, snmp-request
dns-udp	17	53	netmeeting	h323, audio-call-control, t120
eigrp	88	-	network-protocols	dns-tcp, dns-udp, dhcp-server
finger-tcp	6	79	nfs	portmapper-tcp, portmapper-udp, nfsd-tcp, nfsd-udp
ftp	6	21	pptp	pptp-tcp, gre
gopher-tcp	6	70	secure-management	https, ssh
gre	47	-	sip	sip-tcp, sip-udp
h323	6	1720	sms-config	http, https, sms-client, snmp-request, ssh
http	6	80	sms-get	ntp, sms-trap
https	6	443	snmp	snmp-request, snmp-trap
igmp	2	-	vnc	vnc-browser, vnc-viewer
ike	17	500	voice	3com-nbx, sip-tcp, sip-udp
imap	6	143	vpn-protocols	pptp-tcp, l2tp, gre, ike, nat-t-esp
imapv3	6	220		
ipsec-ah	51	-		
ipsec-esp	50	-		
kerberos-tcp	6	88		
kerberos-udp	17	88		
l2tp	17	1701		
ldap-tcp	6	389		
ldap-udp	17	389		

You can complete the following tasks from the Create Firewall Services page:

- Adding a Service to add or change a port and protocol configuration, or to define an arbitrary IP protocol
- Editing a Service to add or change a port and protocol configuration
- Add a Service Group
- Edit a Service Group to add or remove services
- Delete a Service or Service Group



For additional information, see the following topics:

- [“Firewall Service and Service Group Information” on page 77](#)
- [“Adding a Service” on page 77](#)
- [“Editing a Service” on page 78](#)
- [“Configuring Service Groups” on page 78](#)
- [“Add a Service Group” on page 78](#)
- [“Edit a Service Group” on page 79](#)

Firewall Services Page Field Descriptions

The following table describes the fields available on the Firewall Services page.

Table 4–3: Firewall Service and Service Group Information

Column	Description
Firewall Services	
Service	The name of the service. This name displays in the Service dropdown selection list for firewall and virtual interface configuration.
Protocol	The IP protocol used by the service.
Ports	The TCP or UDP port numbers associated with the service, or the ICMP type for services that use the ICMP protocol.
Functions	<p>The functions available for the Services are:</p> <p>Note You cannot edit or delete default Services. You can only edit Services that you have created.</p> <ul style="list-style-type: none">  Edit a Service or Service Group to add or remove services.  Delete a Service or Service Group
Firewall Service Groups	
Service Group	The name of the Service Group. This name displays in the Service dropdown selection list for firewall and virtual interface configuration.
Services	The services associated with the specified group.
Functions	<p>The functions available for Service Groups are:</p> <ul style="list-style-type: none"> Edit a Service or Service Group to add or remove services Delete a Service Group

Adding a Service

STEP 1 On the LSM menu, select **Firewall > Services**.

STEP 2 On the Firewall Services page, click **Add Service** to add a Service.

STEP 3 On the Create Firewall Service page, configure the Service parameters.

STEP A If this is a new Service, type the **Service Name**.

STEP B Select a **Protocol** for the type of connection to be established from the drop-down list.

Depending on the protocol you selected, do one of the following:

- In the **Destination Ports** fields, type the port numbers associated with the service

- From the **Type** drop-down list, select the service type. Protocol types supported are TCP, UDP, ICMP, and IP.
- If the service type is IP, enter the protocol number.

STEP 4 Click **Save**.

Click **Cancel** to return to the Firewall Services page without saving the changes.

Editing a Service

STEP 1 On the LSM menu, select **Firewall > Services**.

STEP 2 On the Firewall Services page, click the service name or **Edit** icon to edit an existing user-defined service.



Note You cannot edit the default services.

STEP 3 On the Edit Firewall Service page, configure the Service parameters.

STEP A Select a **Protocol** for the type of connection to be established from the drop-down list.

Depending on the protocol you selected, do one of the following:

- In the **Destination Ports** fields, type the port numbers associated with the service
- From the **Type** drop-down list, select the protocol type.
- If the service is IP, enter the protocol number.

STEP 4 Click **Save**.

Click **Cancel** to return to the Firewall Services page without saving the changes.

Configuring Service Groups

Service groups allow you to configure a single firewall rule or virtual server to apply to traffic from a collection of services rather than creating individual configurations for each service. After the Service Groups have been configured, you can assign them to firewall rules or virtual servers based on your network security requirements.

For additional information, see the following topics:

- [“Add a Service Group” on page 78](#)
- [“Edit a Service Group” on page 79](#)
- [“Configuring Service Groups” on page 78](#)

Add a Service Group

STEP 1 On the navigation menu, select **Firewall > Services** to open the Firewall Services page.

STEP 2 At the bottom **Firewall Service Groups** table, click **Add Group**.

STEP 3 On the Create Service Group page, type a **Service Group Name**.

STEP 4 For each service you want to add to the group, select the service from the **Service** drop-down list. Then, click the **Add** button.

STEP 5 After adding all services, review the **Service** table to verify the changes.

STEP 6 Click **Create** to save the new Service Group and update the Firewall Services page.

Edit a Service Group

STEP 1 From the LSM menu, select **Firewall > Services** to open the Firewall Services page.

STEP 2 In the **Firewall Service Groups** table, click the name of the Service Group you want to edit.

STEP 3 On the Edit Service Group page, you can either add or delete services:

- To add a service, select a service from the **Service** drop-down list. Then, click the **Add** button.
- To delete a service, locate the service in the table. Then, click the **Delete** icon for the service.



Note You cannot edit or delete default services groups (that is, those with which the device is pre-configured).

STEP 4 Click **Save** to update the Service Group definition.

Schedules

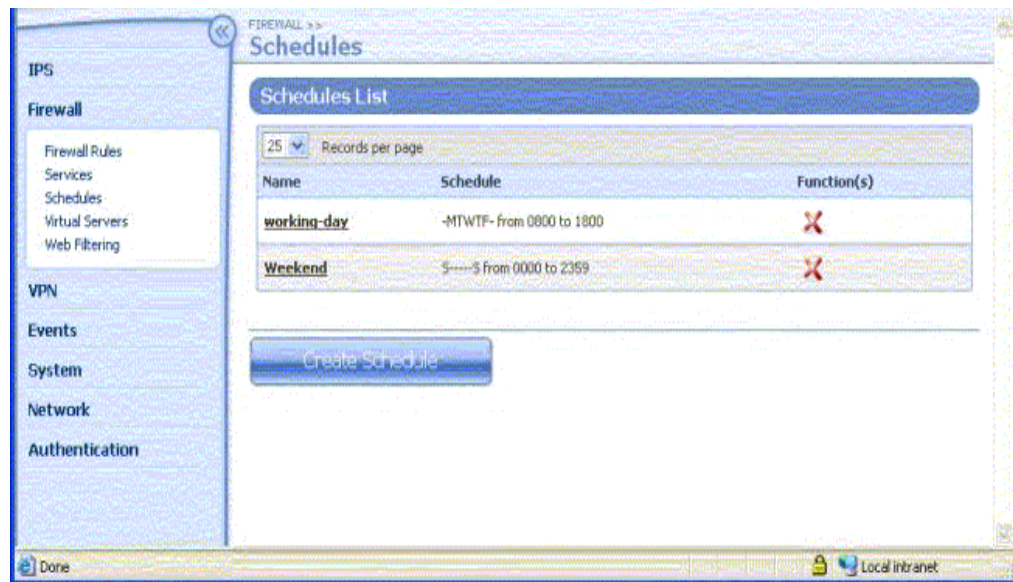
The X family device allows you to create schedules that determine when a firewall rule is in use. Schedules contain intervals of days and hours when the firewall rule applies. For example, Monday to Friday, 8am to 6pm could be a “Work Hours” schedule. The **Always** (default) option can be used if you want the firewall rule to always be applied. Schedules can include multiple entries to specify different time intervals for different days.

You can apply the same schedule to as many firewall rules as required. For device maximum configurable values, see [“Appendix D, “Device Maximum Values”](#).

Use the Schedules page (**Firewall > Schedules**) to view and manage Firewall schedules.

The following figure shows the Schedules page:

Figure 4–4: Firewall: Schedules Page



You can complete the following tasks from the Schedules page:

- Add or Edit a schedule
- Delete a schedule
- Delete Days and Times from an existing schedule



Firewall Schedules Page Field Descriptions

The Schedules page displays and provides the following information about existing schedules:

Table 4–4: Schedules Page: Field Descriptions

Field	Description
Name	The name of the schedule
Schedule	The days and time ranges that define the schedule. Note The value 00:00 is used to specify midnight as either a start or end time.
Functions	The functions available for the Schedules:

Table 4–4: Schedules Page: Field Descriptions (Continued)

Field	Description
	• Edit a schedule to add or remove scheduled time intervals. (Click the linked Schedule name to edit the schedule).
	• Delete a Schedule.

For additional information, see the following topics:

- [“Add or Edit a Schedule” on page 81](#)
- [“Delete Days and Times from an Existing Schedule” on page 82](#)

Managing Schedules

Schedules are only required if you want to configure firewall rules that are only applied to traffic at particular periods of the day, or days of the week. The default schedule for all firewall rules is to always apply, 24 hours, 7 days a week.

When configuring a schedule, select the days of the week that you want to add to the schedule and the time interval (in hours:minutes) during which the schedule will run. You can optionally add multiple day and time interval combinations to the schedule.

For details, see the following topics:

- [“Add or Edit a Schedule” on page 81](#)
- [“Delete Days and Times from an Existing Schedule” on page 82](#)

Add or Edit a Schedule

STEP 1 From the LSM menu, select **Firewall > Schedules**.

STEP 2 On the Schedules page, click the **Create Schedule** button to add a new schedule, or to edit a schedule, click the **Edit** icon for that schedule.



Note You cannot delete or edit default schedules (that is, the schedules with which the device is pre-configured).

STEP 3 On the Create/Edit Schedule page in the **Firewall Schedule** table, type the schedule **Name**.

STEP 4 In the **Schedule Details** table, configure the days and times for the schedule:

STEP A Check the **Days** on which you want the schedule to run.

STEP B To specify the timing for the selected **Days**, select the start time and end time for the schedule in the **Time: From** and **To** drop-down lists.

STEP C Click **Add to table below** to add the schedule.

Repeat Step 4 until you have configured all the required schedules.

STEP 5 Click **Save/Create**.

Click **Cancel** to return to the Firewall - Schedules page without saving the Schedule.

Delete Days and Times from an Existing Schedule

STEP 1 From the LSM menu, select **Firewall > Schedules**.

STEP 2 On the Schedules page in the **Schedule List** table, click the linked Schedule name to access the Edit Schedule page.

STEP 3 In the **Schedule** table, click the **Delete** icon next to the schedule entry you want to delete.

Virtual Servers

You can configure an X family device to deploy what is known as a Virtual Server. A Virtual Server allows you to define a private LAN server IP address for each service passing through the firewall. Any external request for a service, directed at the device's WAN IP address is forwarded to the Virtual Server.

Outgoing sessions from the private server or device to the public network will use the public IP address configured for the Virtual Server. This allows one private IP address to be mapped to one public IP address. If you select *all services* for the service, this provides one-to-one NAT for devices on the private LAN.

In a **one-to-one NAT** configuration, the device uses a pool of Internet IP addresses for Network Address Translation. Each internet IP address is associated with one LAN IP address. Effectively, each of these LAN IP addresses has its own public IP address. By using one-to-one NAT you can allow servers on your LAN, which are protected by the device firewall, to be accessed from the Internet without exposing the internal IP addresses of these hosts on your network to the Internet. Individual PCs can appear to have a public IP address if necessary.

After creating a Virtual server, you must configure firewall rules that allow external devices to access internal servers. You can define a private LAN server IP address for each service passing through the firewall. Any external request for a service, directed at the specified Public IP address of the Virtual Server, is forwarded to the Virtual Server.

For additional information, see the following topics:

- [“Virtual Servers page” on page 83](#)
- [“Configuring Virtual Servers” on page 84](#)

Virtual Servers page



Use the Virtual Servers page (**Firewall > Virtual Servers**) to view and configure Virtual Servers. You can complete the following tasks from this page:

- View a list of existing virtual servers
- Create a virtual server
- Edit/Delete an existing server

Virtual Servers Summary Information

The Virtual Servers page displays and provides the following information about existing Virtual Servers:

Table 4–5: Virtual Servers Summary Information

Column	Description
Service	The name of the Service running on the server.
Public IP	The IP address for users to access the Service, that is, the Virtual Server IP address.
Local IP	The IP address of the server on the LAN to which the Virtual Server is redirecting traffic. Through one-to-one NAT or PAT, accesses to the public IP addresses are changed to accesses to the Local IP address/Port.
Local Port	The port number on which the LAN server is running the Service. Only used if Port Address Translation (PAT) is enabled. For details, see “Virtual Servers Configuration Parameters” on page 84 .
Function(s)	<p>The functions available for the existing Virtual Servers:</p> <ul style="list-style-type: none">  • Edit a the configuration for a Virtual Server. (Click the linked Virtual Server name to edit the schedule).  • Delete a Virtual Server.

For additional information, see the following topics:

- [“Configuring Virtual Servers” on page 84](#)
- [“Configure a Virtual Server and Provide One-to-One NAT” on page 85](#)

Configuring Virtual Servers



For device maximum configurable values, see [“Appendix D, “Device Maximum Values”](#). The following information applies to Virtual Server configuration:

- Virtual Server traffic is subject to firewall rules. You must set up a firewall rule to allow the traffic for the desired services through the device firewall. To allow incoming traffic, use the IP address, or the zone containing the IP address of the LAN device as the destination address of the firewall rule.
- When a Virtual Server is created for *all services* on the external IP interface of the device, all incoming sessions, not otherwise intercepted as other private LAN servers for other services, are directed to the server’s IP address. This configuration will result in loss of management access to the device from the WAN.

Virtual Servers Configuration Parameters

The following table describes the configuration parameters for Virtual Servers.

Table 4–6: Virtual Servers Configuration Parameters


Column	Description
Service	The name of the Services or Service Group that are allowed to run on the Virtual Server.
Local IP	The IP address of the server on the LAN to which the Virtual Server is redirecting traffic. Through one-to-one NAT or PAT, accesses to the public IP address will be changed to accesses to the Local IP address/Port.
Public IP Address	The IP address for users to access the service or group of services, that is, the Virtual Server IP address: <ul style="list-style-type: none"> • Select Use external IP interface address to use the external IP interface address for the device • Select IP address and then type an IP address that is part of the device’s WAN IP subnet, but different from the one the device is currently using.
PAT Local Port	Check PAT to enable Port Address Translation. Then, specify a local port number to map a service to a different local port. Normally, the Service would use its default port number, but PAT or NAPT (Network Address Port Translation) performed by the device allows a user to translate this to a different port number. This would allow, for example, the LAN server to run multiple instances of a Web server.
Function(s)	The functions available for the Virtual Servers: <div>  <ul style="list-style-type: none"> • Edit a the configuration for a Virtual Server. (Click the linked Virtual Server name to edit the schedule). </div> <div>  <ul style="list-style-type: none"> • Delete a Virtual Server. </div>

Configure a Virtual Server and Provide One-to-One NAT

STEP 1 From the LSM menu, select **Firewall > Virtual Servers**.

STEP 2 On the Virtual Servers page, To add a new virtual server, click **Create**. To edit an existing one, click the **Edit** icon for that server.

STEP 3 On the Create/Edit Virtual Server page, select the **Service** that will run on this virtual server.

 **Note** To provide one-to-one NAT to a LAN client, select ALL from the Service drop-down list.

STEP 4 In the **Local IP Address** field, enter the IP address of the server on the LAN to which you want traffic redirected.


For one-to-one NAT, this address is the LAN client address.

STEP 5 For the **Public IP Address**, either:

- Select **Use External interface IP address**.
- Select **IP Address**. Then, type a public IP Address that is different from the X family device public WAN IP Address.


This option can only be used if you have been provided with multiple IP addresses. You must select this option for one-to-one NAT.

STEP 6 If you want a default port number used by the service to be translated to a different port number by the X family device, check **Enable PAT** and enter the port number you want in the **Local Port** field.

 **Note** The Enable PAT checkbox and the Local Port field are disabled if you have selected ALL from the Service drop-down list.

STEP 7 Click **Create**.

Click **Cancel** to return to the FIREWALL - Virtual Servers page without saving the changes.

 **Note** Virtual Server traffic is subject to firewall rules. You must set up a firewall rule to allow the traffic for the desired services through the firewall. To allow incoming traffic, use the IP address, or the zone containing the IP address, of the LAN device as the destination address of the firewall rule.

Web Filtering

The options on the **Web Filtering** menu in the LSM enable you to view and change configuration for web filtering (sometimes known as content filtering). Web filtering allows you to control access to Web sites from the X family device. The device supports both **custom filtering** and filtering using the **Web Filter Service**.

- **Custom filtering** enables you to permit or block access to different Web sites based on their URLs, domain names, IP addresses, pattern matching, or keyword matching. No content categorization is

used to determine whether a Web site may be accessed or not. You must specify all rules to permit or block access to specific Web sites.

- **Web Filter Service** is a subscription service that provides filtering based on classifications of Web sites. Web sites are classified into Core Categories or Productivity Categories. You control Web site access by permitting or blocking access to these categories.

If you apply both types of filtering, custom filters takes precedence over Web Filter category filters. Therefore, you can use a custom filter to override the Web Filter Service for a particular web site.



Note For the X family device to use Web filtering, you must set up a firewall rule with an action of “Web Filter.” This rule must be positioned in the firewall rule table to ensure it matches the web traffic before any other rule that would also allow Web traffic (a “permit LAN==>WAN ANY” rule, for example). For more information about firewall rules, see [“How Firewall Rule Enforcement Works” on page 64](#).

On the X family device, user authentication can be implemented in conjunction with firewall rules to allow selected users to bypass web filtering. User authentication is a method of verifying the identity of a user and associating the user with privilege rights configured on the device. For example, if you want to allow a certain group of users unrestricted access to all Web sites, you can assign those users to a Privilege Group with access rights to *bypass web filtering*. For details, see [“How Local User Authentication Works: RADIUS, Privilege Groups and X.509 Certificates” on page 251](#).

For additional information, see the following topics:

- [“How Web Filtering Works” on page 86](#)
- [“How Local User Authentication Works: RADIUS, Privilege Groups and X.509 Certificates” on page 251](#)
- [“Setting Up Web Filtering” on page 87](#)
- [“Custom Filter List” on page 92](#)
- [“Web Filter Service” on page 90](#)
- [“Web Filter Service” on page 281](#)

How Web Filtering Works

The following description provides an overview of how a client request is handled by X family device for Web filtering.

- STEP 1** The browser forms a connection to the desired web site. It then issues an HTTP GET request over the connection. The device inspects the session header of the request and identifies the IP address of the pc running the web browser.
- STEP 2** The device checks whether there is a user logged in from this PC with *Bypass web filtering* as a user privilege. If so, the request is served and access is permitted.
- STEP 3** The device checks whether the Custom Filter list options are enabled. If so, it checks the Custom Filter URL Permit List for a pattern match. If there is a match, the request is served and access is allowed.
- STEP 4** If there is no match in the URL Permit List, the device checks the URL Block List for a pattern match. If there is a match, the filter blocks the request.

- STEP 5** If there is no pattern match in the URL Block List, the device checks to see if the Web Filter Service is licensed and enabled. If it is enabled, the device contacts the Web Filter Service server to determine if the URL matches a category included in the Web Filter Service database. If a match is found in a blocked category, the request is filtered executing the action configured for the Web Filter Service: block only, log only, block and log. If a match is found in a permitted category, the request is served and access is allowed.



Note A local cache is available for the Web Filter Service to speed up the filtering process.

- STEP 6** If the request is not a member of a currently filtered category or covered by an entry in the Custom Filter List, the Web Filter Service is not licensed, or the CPA Server cannot be contacted by device, the web filtering default rule is applied. The default rule can be configured with one of the following actions:

- **Allow unclassified or unknown sites**
- or
- **Filter unclassified or unknown sites** - which means the filtering action that you specify will be applied

- STEP 7** If the firewall web-filter rule has logging enabled, and the device denies access to a web site based on the Custom Filter List or the Web Filter Service, a “Warning” level Security event is sent to the Firewall Block Log. For allowed requests, “Informational” events are logged in the Firewall Session Log.

For additional information, see the following topics:

- [“Setting Up Web Filtering” on page 87](#)
- [“Web Filtering Page” on page 88](#)
- [“Web Filter Service” on page 90](#)
- [“Custom Filter List” on page 92](#)

Setting Up Web Filtering

The following steps provide an overview of the web filter configuration process:

- STEP 1** Configure general web filtering settings. These settings determine the device response to web requests when the Web Filtering options are enabled.
- For details, see [“Web Filtering Page” on page 88](#)
- STEP 2** If you are using the Web Filter Service, configure the Web Filter Service settings.
- For details, see [“Web Filter Service” on page 90](#).
- STEP 3** If you are using the Custom Filter List, configure the Permit and Block URL lists.
- For details, see [“Custom Filter List” on page 92](#).
- STEP 4** Configure a firewall rule to apply web filtering.
- For details, see [“Configuring Firewall Rules” on page 71](#).

If you create a Custom Filter, can select the **Create default firewall rule** option to automatically generate the web filtering firewall rule. However, you will have to reposition the rule to the top of the firewall rule table after it has been generated.

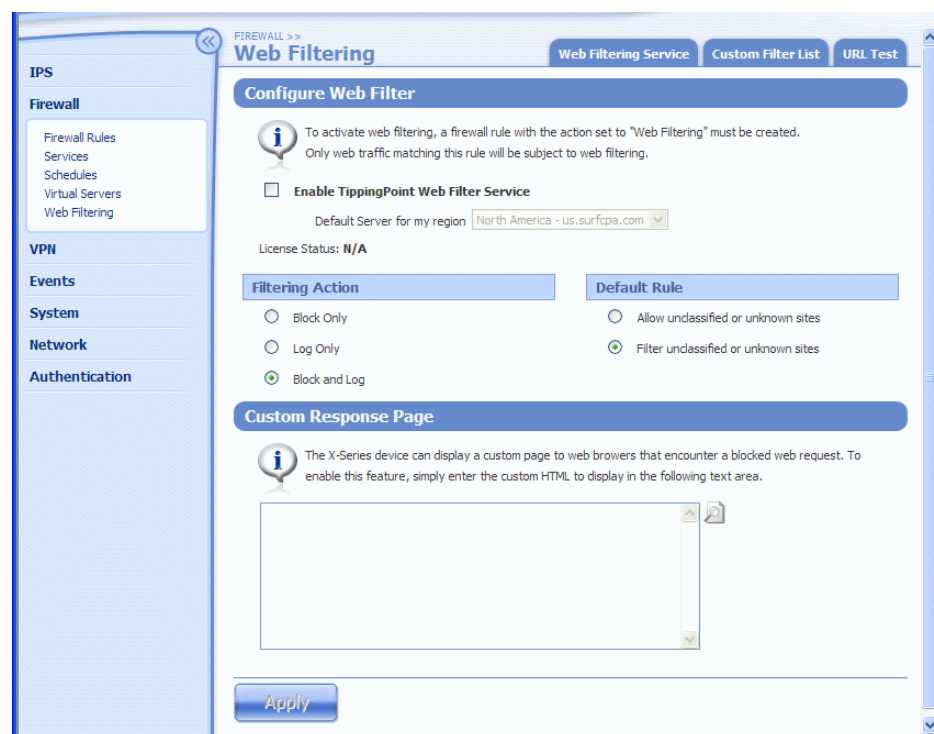
STEP 5 Configure user privileges to bypass web filtering (optional).

For details, see [“Create/Edit a Privilege Groups” on page 254](#).

Web Filtering Page

Use the Web Filtering menu page (**Firewall > Web Filtering**) to enable, configure and manage the Web Filter functions available on X family devices. The following figure shows the Web Filtering page.

Figure 4–5: Firewall Rules: Web Filtering: Configure Web Filter



You can complete the following tasks from the Web Filtering page:

- Enable/disable the Web Filtering subscription service
- Define the default filtering action for web filter block events
- Specify the default behavior (known as Default Rule) for managing web requests for sites that are not included in either the filters defined by the Web Filter Service filters or the URL lists defined in the Custom Filter List, or if the Web Filter Service is unavailable or unlicensed.
- Create a custom response page to display when a web request is blocked. This page is returned to the web browser that made the web request.
- Access configuration and management functions for the Web Filter Service and the Custom Filter List.

For details, see the following topics:

- [“Web Filter General Configuration Parameters” on page 89](#)
- [“Configure Web filtering” on page 89](#)
- [“Web Filter Service” on page 90](#)
- [“Custom Filter List” on page 92](#)

Web Filtering General Configuration Parameters

The following table describes the general configuration parameters to enable and configure the Web Filter functions available on X family devices. In addition to these parameters, you must also make sure that the device has the following items configured: a valid DNS server and default gateway (**Network > Configuration**), and the web filter firewall rules (**Firewall > Firewall Rules**).


Table 4–7: Web Filter General Configuration Parameters

Parameter	Description
Configure Web Filter	Determines whether the Web Filter Service is enabled or disabled. If the service is enabled, specify the Default Server for my region . The License Status field indicates the status of the license for the Web Filter Service. To configure the Web Filter Service filters, use the Web Filtering Service tab.
Filtering Action	Determines the system logging behavior for web requests blocked by filters in the Web Filtering Service or the Custom Filters List.
Default Rule	If web filtering is enabled, these options determine how the device handles web requests for sites that are not covered by filters in the Web Filter Service or the Custom Filter list. The following options are available: <ul style="list-style-type: none"> • Allow unclassified or unknown sites. • Filter (Block) unclassified or unknown sites
Custom Response Page	Specifies a custom message that will be added to the standard access blocked Web page that displays when a web request is blocked by a web filter. You can use the following custom tags in the message: <ul style="list-style-type: none"> • %category% to display the category the blocked page falls under • %url% to display the URL of the blocked page

Configure Web filtering

STEP 1 From the LSM menu, select **Firewall Rules > Web Filtering**.

STEP 2 To use the Web Filtering Service, check **Enable Web Filter Service**.

- STEP 3** In the **Filtering Action** table, configure the behavior for web filter events. This configuration determines how the device handles logging for blocked web requests. Select one of the following:
- To block requests without creating entries in the Firewall Block Log even if the web filter firewall rule has logging enabled, select **Block Only**.
 - To permit the requests and record them in the Firewall Block Log, select **Log Only**.
 - To both block the requests and log any attempts in the Firewall Block Log, select **Block and Log**.
- STEP 4** In the **Default Rule** table, configure the behavior to handle web requests for sites that are not covered by filters in the Web Filter Service or the Custom Filter list. Select one of the following:
- To allow these requests, select **Allow unclassified or unknown sites**.
 - To filter these requests, select **Filter unclassified or unknown sites**.
- STEP 5** To display a custom message (in addition to the standard access blocked message) when a web request is blocked by a web filter:
- Type the message in HTML in the **Custom Response Page** section.
 - Click  **Preview** to check that the message displays correctly.
- STEP 6** Click **Apply** to save and apply the general filtering configuration.

Web Filter Service

The Web Filter Service is a subscription content filtering service that provides web content filtering based on web site classifications. This service is operated in partnership with SurfControl, a leading provider of content filtering solutions. The URL database has over 5 million entries and contains URLs

in a variety of languages (65 languages) from over 200 countries. Web sites are classified into two main categories:

- **Core Categories** cover web sites that contain offensive, potentially dangerous, or criminal content.
- The Web Filter Service blocks URLs that are included in any Core category by default. If necessary, you can change the default setting for any category to allow access. For a list of the category types, see [“Core Categories” on page 282](#).
- **Productivity Categories** cover websites that could impair productivity when used in the work environment.

The Web Filter Service allows URLs that are included in any Productivity category by default. If necessary, you can change the default setting for any category to block access. For a list of the category types, see [“Productivity Categories” on page 284](#).

The Web Filter Service is a subscription-based service which requires the purchase of the correct license for your product from a reseller. For details, see [“Purchasing a Web Filter License” on page 289](#).

You can configure the Web Filter Service Category settings from the Web Filtering Service page shown in the following figure:

Figure 4–6: Firewall: Web Filtering: Web Filtering Service Page

The screenshot shows the 'Web Filtering Service' configuration page. On the left is a sidebar with navigation links: IPS, Firewall, VPN, Events, System, Network, and Authentication. The 'Firewall' section is expanded, showing sub-links: Firewall Rules, Services, Schedules, Virtual Servers, and Web Filtering. The main content area has a breadcrumb trail 'FIREWALL >> WEB FILTERING >>' and a title 'Web Filtering Service'. Below the title is a note: 'To activate the web filtering, a firewall rule with the action set to "Web Filter" must be created. Only web traffic matching this rule will be subject to web filtering.' There are three tabs: 'Web Filtering Service' (selected), 'Custom Filter List', and 'URL Test'. The 'Core Categories' section has the instruction 'Select the core categories to be allowed.' and lists categories with checkboxes: Adult/Sexually Exploit, Criminal Skills, Drugs, Alcohol & Tobacco, Gambling, Hacking, Hate Speech, Violence, and Weapons. The 'Productivity Categories' section has the instruction 'Select the productivity categories to be allowed.' and lists categories with checkboxes: Advertisement, Arts & Entertainment, Chat, Computing & Internet, Education, Finance & Investment, Food & Drink, Games, Glamour & Intimate Apparel, Government & Politics, Health & Medicine, Hobbies & Recreation, Hosting Sites, Job Search & Careers, Sites for Children, Lifestyle & Culture, Motor Vehicles, News, Personals & Dating, Photo Searches, Real Estate, Reference, Religion, Remote Proxies, Sex Education, Search Engines, Shopping, Sports, Streaming Media, Travel, Usenet News, and Web-based Email. Each category has a checkbox, and many are checked.

Configure Web Filter Service Categories

STEP 1 From the LSM menu, select **Firewall > Web Filtering Content Categories**. Then, click the **Web Filtering Service** tab.

STEP 2 To configure filters in the **Core Categories** table:

STEP A Clear the check box next to a category name to *allow* access. To block access, check the check box next to the category name.

STEP B Click **Apply** to save changes and apply the filtering.

STEP 3 To configure filters in the **Productivity Categories** table:

STEP A To *block* access, clear the check box next to the category name. To *allow* access, check the check box next to the category name.

STEP B Click **Apply** to save changes and apply the filtering.

After enabling and configuring the Web Filter Service, use the URL Test page to determine the filter category for a specific URL.

Custom Filter List

Use the Custom Filter List menu pages to create URL Permit or Block lists consisting of lists of URL name patterns which can represent domain names, URLs, IP addresses, simple keywords or regular expressions entered by the administrator. When a user requests a connection to a website, the device checks the URL address against the addresses included in the Current Permit Patterns and Current Block Patterns to see if the user is permitted to view the site.

The X family device performs a DNS to IP address conversion before checking the Permit/Block lists. This enables web sites to be identified by domain or IP address, and prevents the Block List from being undermined by web requests for its IP address.

Use the Custom Filter List page (**Firewall > Web Filtering**) to configure and manage the Permit and Block lists. The following figure shows the Custom Filter List page.

Figure 4–7: Firewall: Web Filtering: Custom Filter List Page

The screenshot shows the 'Custom Filter List' page under 'Firewall >> WEB FILTERING >>'. The page has a sidebar with navigation links: IPS, Firewall, VPN, Events, System, Network, and Authentication. The main content area is divided into several sections:

- General Configuration:** Includes checkboxes for 'Enable Manual URL Filtering' (checked) and 'Create default firewall rule' (checked), with an 'Apply' button below.
- Add URL Pattern:** A section for adding new patterns. It includes a radio button for 'Permit' (selected) and a radio button for 'Block'. Below is a text input for 'URL Pattern' and a checkbox for 'Regular Expression'. An 'Add >' button is at the bottom.
- Current Permit Pattern(s):** A table showing the current permit patterns. It has two columns: 'Pattern' and 'Function(s)'. The table is currently empty.
- Current Block Pattern(s):** A table showing the current block patterns. It has two columns: 'Pattern' and 'Function(s)'. The table contains four entries, each with a red 'X' in the 'Function(s)' column:

Pattern	Function(s)
www.msn.com	X
www.yahoo.com	X
www.fortune.com	X
http://blackice.iss.net/update_center/readme_pcp.txt	X
- Import URL Lists:** Includes a 'File to Import' text input, a 'Browse...' button, and radio buttons for 'Overwrite existing URL lists' (selected) and 'Merge with existing URL lists'. An 'Import' button is at the bottom.
- Export URL Lists:** Includes an 'Export' button and a note: 'the URL lists to a text file.'

You can complete the following tasks from the Custom Filter List page:

- Enable/disable Manual URL filtering using the Custom Filter List
- Create a default firewall rule with a web filter action
- Create Permit/Block Lists
- Delete a URL from the Permit/Block List
- Import the Permit and Block List from another X family device
- Export the Permit and Block List from the current device to a file

Custom Filter List Configuration Parameters and Functions

The following table describes the configuration parameters and functions available on the Custom Filter List page (**Firewall > Web Filtering**).

Table 4–8: Custom Filter List Page: Configuration Parameters and Functions

Parameter/Function	
Enable Manual URL Filtering	Enables/Disables the feature to block or permit traffic based on a Custom Filter list
Create default firewall rule	Custom web filter
Action	Permit or Block
URL Pattern	Block or permit traffic to/from a group based on a URL name pattern. For details, see “Configure URL Patterns” on page 94 .
Import Function	If you have exported a the Custom Filter List from another X family device, use the import function to upload the list to the X family device.
Export Function	Use the Export feature to download the current Permit and Block Pattern lists so that you can import them to another X family device.
Delete Function	Use the Delete icon in the Current Permit Pattern and Current Block Pattern table, to remove a URL pattern from the list.

Configure the Custom Filter List

STEP 1 From the LSM menu, select **Firewall Rules > Web Filtering**. Then, select the **Custom Filter List** tab.

STEP 2 On the Custom Filter List, select the General Configuration parameters:

STEP A To use the custom Permit/Block lists to control access to web sites, click **Enable Manual URL Filtering**.

STEP B To create a default firewall rule for web filtering, click **Create default firewall rule**.

STEP C Click **Apply**.

STEP 3 Create and add the URL patterns to the Permit/Block lists:

STEP A In the **Add URL Pattern** table, select the **Action** to take when a web request matches the pattern: **Permit** or **Block**.

STEP B Type or edit the **URL Pattern** you want to match.

If you are using a regular expression, check the **Regular Expression** check box. For details on creating regular expressions, see [“Configure URL Patterns” on page 94](#).

STEP C Click **Add**.

The pattern is added to the **Current Patterns** table for the selected action (permit or block).

Delete a Pattern in the Permit or Block List

STEP 1 From the LSM menu, select **Firewall Rules > Web Filtering**. Then, select the **Custom Filter List** tab.

STEP 2 On the Custom Filter List page, in the **Current Permit Pattern(s)** or **Current Block Pattern(s)** **lock List**, table, click the **Delete** icon for the entry to delete.

STEP 3 On the confirmation pop-up, click **OK** to delete the pattern and update the list.

Import URL Lists

STEP 1 From the LSM menu, select **Firewall Rules > Web Filtering**. Then, click the **Custom Filter List** tab.

STEP 2 On the Custom Filter List page in the **Import URL Lists** table, type the filename and path for the File to Import, or click **Browse** and navigate to the file.

STEP 3 Choose the Operation you want to perform when importing the list, either:

- Select **Overwrite existing URL lists** to delete the existing URL Lists and replace them with the imported lists.
- Select **Merge with existing URL lists** to add the imported URL Lists to the existing lists.

STEP 4 Click **Import** to import the custom filter list file to the X family device.

Export URL Lists

STEP 1 From the LSM menu, select **Firewall Rules > Web Filtering**. Then, click the **Custom Filter List** tab.

STEP 2 On the Custom Filter List page in the **Export URL Lists** table, click **Export** to save the custom filter rule list to a file.

STEP 3 On the Custom Filter List page in the **Export URL Lists** table, click **Export**. Then, save the resulting Custom Filter list text file.

Configure URL Patterns

Requests for access to Web sites can be permitted or blocked depending on whether the requested URL matches a pre-set pattern.

A **Pattern** can be a domain name, a URL, an IP address, a simple keyword or a regular expression.

Regular expression pattern matching enables you to enter regular expressions into the Permit/Block lists to identify URLs. URL patterns that match these expressions are either permitted or blocked.

The simplest use of pattern matching is to implement keyword blocking, where any URL containing a keyword will be blocked regardless of its categorization.

A valid regular expression must be between 3 and 64 characters in length, and conform to the full regular expression syntax.

Examples of patterns are:

http://www.Acme.com — URL, to match the protocol.

www.Acme.com — keyword, to match the Acme site only.

www.Acme.com/* — a pattern to match any page on the Acme site.



Note You can use the wildcard (*) character anywhere in your entries into the URL Permit and Block Lists. The wildcard (*) character is allowed with or without the Regular Expression checkbox ticked. It is interpreted as zero or more characters. Wildcards are not implicitly added to the front and end of the string, thus allowing you to specify an absolute URL or a wildcard URL. Note that all matches are case insensitive.

Examples of regular expression patterns are shown in the table below:

Table 4–9: Regular Expression Syntax

Value	Description
x	Matches the character x
.	Match any character
^	Specifies beginning of line
\$	Specifies end of line
[xyz]	A character class. In this case, the pattern matches either x, y, or z
[abj-oZ]	A character class with a range. This pattern matches a, b, any letter from j through o, or Z
[^A-Z]	A negated character class. For example, this pattern matches any character except those in the class
r*	Zero or more r's, where r is any regular expression
r+	One or more r's, where r is any regular expression
r?	Zero or one r, where r is any regular expression
r{2,5}	From two to five r's, where r is any regular expression
r{2,}	Two or more r's, where r is any regular expression
r{4}	Exactly 4 r's, where r is any regular expression

Value	Description
"[xyz]"images"	The literal string [xyz]"images"
\x	If x is a, b, f, n, r, t, or v, then the ANSI-C interpretation of \x; Otherwise, a literal X. This is used to escape operators such as *.
\0	A NULL character
\123	The character with octal value 123
\x2a	The character with hexadecimal value 2a
(r)	Matches an r; where r is any regular expression. You can use parentheses to override precedence
Rs	The regular expression r, followed by the regular expression s
r s	Either an r or an s
#<n>#	Inserts an end node causing regular expression matching to stop when reached. The value n is returned

URL Test

Use the **URL Test** dialog to determine if a URL is covered by one of Web Filter Service category filters.

Check the Category of a URL

STEP 1 From the LSM menu, select **Firewall > Web Filtering**. Then, select the URL Test tab.

STEP 2 On the URL Test page in the **Test URL** table, type the URL you want to check.

STEP 3 Click **Test** to display the result.

One of the following messages displays:

- A message showing the category for the URL, for example:
`www.bbc.co.uk is in the News Productivity Category`
- `Error. Unable to contact categorization server`
 This message refers to the server selected on the Web Filtering page. To resolve the error:
 - Verify the X family DNS configuration specified on the device
 - Check general Internet connectivity.
 - Verify that the DNS configuration settings (**Network > Configuration > DNS**) on the external (WAN) virtual interface.
- `Error. Device is not licensed to use the 3Com web-filter service.`
 Purchase or renew the subscription for the Web Filter Service.

5

Events: Logs, Traffic Streams, Reports

The Events section describes the logs, views and reports available to monitor system performance and traffic-related events triggered by firewall rules, web filters, IPS filters and traffic threshold policies. In this section, you will review the information presented in the Events pages and learn how to manage the logs and reports. Only users with Super-user access may view all of the logs and reports available.

Overview

The Events menu pages of the LSM allow you to monitor system performance and review traffic-related events. The menu provides the following options:

- **Logs** — View information on system events and traffic-related events triggered by firewall, IPS, and traffic threshold security policies.
- **Managed Streams** — Review and manage traffic streams that have been blocked, rate-limited, or quarantined by IPS policies. You can also manually quarantine or release a quarantined IP address.
- **Health** — Review the current status and network performance of the X family device. Information includes memory and disk usage statistics, status of the Threat Suppression Engine and the Ethernet ports, and throughput performance.
- **Reports** — View graphs showing information on traffic flow, traffic-related events, and statistics on firewall top sites, top services, top clients, rule hit counts, and triggered filters (attack, rate limit, traffic threshold, quarantine, and adaptive filter).

For details, see the following sections:

- [“Logs” on page 98](#)
- [“Managed Streams” on page 110](#)
- [“Health” on page 116](#)
- [“Reports” on page 121](#)

Logs

The Logs menu pages provide information on system events and traffic-related events triggered by firewall, IPS, and traffic threshold security policies. Each menu page also provides functions to manage the log files.

When you review logs, you may also see the following type of administrator user levels. These users denote the type of account according to the interface they used in the device:


- **SMS** — Indicates the administrator used the SMS when the messages saved to the logs
- **LSM** — Indicates the administrator used the LSM when the messages saved to the logs
- **CLI** — Indicates the administrator used the CLI when the messages saved to the logs



Note Users with any access level can view and print the system log, but only Administrator and Super-user level users can reset this log.

Log Maintenance

The X family device maintains two files for each log: a historical log file and a current log file. When the current log file reaches the default size (4MB), the log is de-activated and saved as the historical file. A new log file is started as the current log. If a historical file already exists, that file is deleted. When the log is rolled over, the device generates a message in the Audit log. To save log all data and create a backup, configure the device to offload log messages to a remote system log.

You can reset a log from its menu page, or use the Reset  function available on the System Summary page.

For details, refer to the following sections:

- [“Alert Log” on page 99](#)
- [“Audit Log” on page 100](#)
- [“IPS Block Log” on page 101](#)
- [“Firewall Block Log” on page 102](#)
- [“Firewall Session Log” on page 103](#)
- [“VPN Log” on page 104](#)
- [“System Log” on page 105](#)
- [“Managing Logs” on page 106](#)
- [“Configuring Remote System Logs” on page 105](#)

Alert Log

The Alert log contains information about network traffic that triggers IPS filters configured with a Permit + Notify or Permit+Notify+Trace action set. Any user can view the log, but only administrator and super-user level users can print the log.

To maintain a complete history of entries and provide a backup, you can configure the X family device to send Alert Log entries to a remote syslog server from the Notification Contacts page. For details, see [“Notification Contacts” on page 52](#).

An Alert log entry contains the following fields:

Table 5–1: Alert Log Field Descriptions

Column	Description
Log ID	A system-assigned Log ID number
Date/Time	A date and time stamp in the format year-month-date hour:minute:second
Severity	Indicates the severity of the triggered filter. Possible values include: Critical, Major, Minor, and Low
Filter Name	The name of the IPS filter that was triggered
Protocol	The name of the protocol that the action affects
Security Zone (pair)	The Security Zone pair where the alert occurred (LAN -WAN, for example)

Table 5-1: Alert Log Field Descriptions (Continued)

Column	Description
Source Address	The source address of the triggering traffic
Dest Address	The destination address of the triggering traffic
Packet Trace	Details if a packet trace is available
Hit Count	Details how many packets have been detected

Audit Log

The audit log tracks user activity that may have security implications, including user attempts (successful and unsuccessful) to do the following:

- Change user information
- Change IPS, firewall, routing or network configuration
- Gain access to controlled areas (including the audit log)
- Update system software and attack protection filter packages
- Change filter settings



Note Only users with Super-user access level can view, print, reset, and download the audit log.

To maintain a complete history of entries and provide a backup, you can configure the X family device to send Audit Block Log entries to a remote syslog server from the Syslog Servers page. For details, see the [“Syslog Servers” on page 242](#).

An Audit log entry contains the following fields:

Table 5-2: Audit Log Field Descriptions

Column	Description
Log ID	A system-assigned Log ID number
Date and Time	A date and time stamp in the format year-month-date hour:minute:second
Username	The login name of the user performing the action. The user listed for an event may include SMS, SYS, and CLI. These entries are automatically generated when one of these applications performs an action.
Access Level	The access-level of the user performing the action
IP Address	The IP address from which the user connected to perform the action
Interface	The interface with which the user logged in (either WEB for the LSM or CLI for the Command Line Interface)

Table 5-2: Audit Log Field Descriptions (Continued)

Column	Description
Component	The area in which the user perform an action (LOGIN, LOGOUT and Launch Bar Tabs)
Result	The action performed or the result of a LOGIN or LOGOUT attempt
Action	The action performed as a result. For example, Log Files Reset.

IPS Block Log

The IPS Block log contains information about packets that have triggered an IPS filter configured with a Block + Notify action set.

To maintain a complete history of entries and provide a backup, you can configure the X family device to send IPS Block Log entries to a remote syslog server from the Notification Contacts page. For details, see the [“Notification Contacts” on page 52](#).

An IPS Block log entry contains the following fields:

Table 5-3: IPS Block Log Field Descriptions

Column	Description
Log ID	A system-assigned Log ID number
Date/Time	A date and time stamp in the format YYYY-MM-DD HH:MM:SS
Severity	Indicates the severity of the triggered filter. Possible values include: Low = 1 Minor = 2 Major=3 Critical=4 Note When the log is downloaded, the Severity value is reported using the numerical value.
Filter Name	The name of the filter that was triggered
Protocol	The name of the protocol that the action affects
Security Zone (pair)	The Security Zone pair where the alert occurred (LAN to WAN, for example)
Source Address	The source address of the triggering traffic
Dest Address	The destination address of the triggering traffic
Packet Trace	Details if a packet trace is available
Hit Count	Details how many packets have been detected

Firewall Block Log

The Firewall Block Log captures information about events that have triggered a firewall rule that blocks matching traffic and has logging enabled.

A log entry is generated for each of the following events.

- Block web request event: occurs when the X family device blocks a web request due to web filtering
- Block event: occurs when a firewall rule with Block action is triggered.

To maintain a complete history of entries and provide a backup, you can configure the X family device to send Firewall Block Log entries to a remote syslog server from the Notification Contacts page. For details, see [“Notification Contacts” on page 52](#).

Each log entry is tab-delimited. The log fields are populated based on the type of event being logged. If a field is not used, a tab is inserted to properly position the data in the next field.

A Firewall Block log entry contains the following fields:

Table 5–4: Firewall Block Field Descriptions

Column	Description
Log ID	A system-assigned Log ID number
Date/Time	A date and time stamp in the format YYYY-MM-DD HH:MM:SS
Severity	Indicates the severity of the triggered filter. Possible values include: Critical, Major, Minor, and Low
Firewall Rule	The name of the firewall rule that was triggered. In the LSM, the firewall rule is linked to allow you to edit/view the rule that triggered the event.
Protocol	The name of the protocol that the action affects
Source Zone	The security zone where the traffic originated
Dst Zone	The security zone where traffic was sent
SourceIP: Port Dest	The source address and port where the triggering traffic originates
Dest IP: Port	The destination address and port of the triggering traffic
Category	For web requests blocked by the Web Filter Service, this represents the filter category triggered by the URL (examples: Gambling, Entertainment, or Violence)
URL	For web requests events only, the target URL. This field is populated regardless of whether the request was filtered by the Web Filter Service

Firewall Session Log

For firewall and web filter permit rules with logging enabled, this log captures information on session creation and termination, including the time the session started, and the URL being accessed (for web requests). When a session terminates the Firewall Session Log shows how many bytes were transferred through the session.

A log entry is generated for each of the following events if the firewall rule had logging enabled.

- Web Request event: occurs when the X family device permits a web request to pass through.
- Session Started event: occurs when a firewall rule is triggered.
- Session Close event: occurs when the network connection is ended or closed due to inactivity.

To maintain a complete history of entries and provide a backup, you can configure the X family device to send Firewall Session Log entries to a syslog server from the Syslog Servers page. For details, see the [“Syslog Servers” on page 242](#).

Each log entry is tab-delimited. The log fields are populated based on the type of event being logged. If a field is not used, a tab is inserted to properly position the data in the next field.

A Firewall Session log entry contains the following fields:

Table 5–5: Firewall Session Log Field Descriptions

Column	Description
Log ID	A system-assigned Log ID number
Date/Time	A date and time stamp in the format YYYY-MM-DD HH:MM:SS.
Rule	The ID of the firewall rule triggered.
Protocol	The name of the protocol associated with the session in the format x(y) where: x=protocol name, y=protocol number
Src Zone	Name of the source security zone for the firewall rule
Dst Zone	Name of the destination security zone for the firewall rule.
SourceIP: Port	The source IP address and port from which the session was started
DestIP: Port	The destination IP address and port that is the target of the session
Category	For web requests filtered by the Web Filter Service, this represents the filter category triggered by the URL (examples: Gambling, Entertainment, or Violence)
URL	For web requests blocked by a web filter firewall rule with logging enabled, this field specifies the target URL. This field is populated regardless of whether the request was filtered by the Web Filter Service.
Session Duration(s)	For Session End events only, this field contains the duration of the session based on the session start time. The duration is displayed in the format: DD:HH:MM:SS.

Table 5–5: Firewall Session Log Field Descriptions (Continued)

Column	Description
Bytes	For Session End events, this field contains the number of bytes transferred during each session. For web request events, this field indicates the number of bytes downloaded from the HTTP GET.
Message	Message text associated with the firewall session event: Web request — no message Session start — Regular session start, Secondary session start Session end — Session ended because of inactivity, Session ended because of inactivity

VPN Log

The VPN log captures diagnostic messages relating to VPN tunnels to help troubleshoot and monitor VPN configurations. Each log entry is tab-delimited. The log fields are populated based on the type of event being logged. If a field is not used, a tab is inserted to properly position the data in the next field.

To maintain a complete history of entries and provide a backup, you can configure the X family device to send VPN Log entries to a syslog server from the Syslog Servers page. For details, see [“Syslog Servers” on page 242](#).

A VPN log entry contains the following fields:

Table 5–6: VPN Log Field Descriptions

Column	Description
Log ID	A system-assigned Log ID number
Log Entry Time	A date and time stamp in the format year-month-date hour:minute:second
Severity	The severity of the event, which is INFO.
Src IP:Port	Source address — the IP address and port for the event. This is a string and the value may be <i>this-device</i> , indicating that the X family device sent the message itself.
Dest IP:Port	Destination IP address and port for the event
Message	Free-form text with error messages or notification about a VPN tunnel

Configuration

The logging level for the VPN log can be configured to provide more/less detailed information by configuring the **Enable Verbose** messages in the VPN Log option available on the IPSec Configuration page in the LSM application.

System Log

The System Log contains information about the software processes that control the X family device, including startup routines, run levels, and maintenance routines. System log entries can provide useful troubleshooting information if you encounter problems with the device.

To maintain a complete history of entries and provide a backup, you can configure the device to send System Log entries to a syslog server from the Syslog Servers page. For details, see [“Syslog Servers” on page 242](#).



Note Users with any access level can view and print the system log, but only Administrator and Super-user level users can reset this log.

For information on Adaptive Filter messages, see [“Adaptive Filter Configuration” on page 60](#).

System Log entries are only sent to the syslog server after the device has fully booted. During the boot sequence, entries cannot be sent because network ports are not yet enabled. When the boot sequence completes, the device sends a startup message to the syslog server.

A System log entry contains the following fields:

Table 5-7: System Log Field Descriptions

Column	Description
Log ID	A system-assigned Log ID number
Log Entry Time	A date and time stamp in the format year-month-date hour:minute:second
Severity Level	The severity level of a message indicates whether the log entry is simply informational (INFO) or whether it indicates an error condition (ERR or CRIT)
Component	The component is an abbreviation that indicates which software component sent the message to the log
Message	The message is the text of the log entry

Configuring Remote System Logs

All information logged by the LSM can be offloaded to a remote syslog server. Options to configure logging behavior for traffic-related events are available from the Edit Action Sets page (**IPS > Action Sets > Edit**) and the Edit Firewall Rule page. In order to use remote logging options, you must configure the contact information for the remote syslog servers.

For details on configuring the Remote System Log contact for the Alert, IPS Block, and Firewall Block log messages, see [“Configure the Remote System Log Contact” on page 54](#).

For details on configuring the Syslog Server contact for the System, Audit, VPN, and Firewall Session log, see [“Configure remote syslog for the System, Audit, VPN, and Firewall Session logs” on page 106](#).



CAUTION Remote syslog, in adherence to RFC 3164, sends clear text log messages using the UDP protocol with no additional security protections. Therefore, you should only use remote syslog on a secure, trusted network to prevent syslog messages from being intercepted, altered, or spoofed by a third party.

Configure remote syslog for the System, Audit, VPN, and Firewall Session logs




STEP 1 From the LSM menu, select **System > Configuration > Syslog Servers**.

STEP 2 On the Syslog Servers page, for each log type you want to offload, click the check box and specify the IP address for the syslog server.

Managing Logs

On each log page, the functions available for the log are displayed at the top of the page. You can also access the log functions from the System Summary page. The following table describes these functions:

Table 5–8: Log Functions

Function	Icon/Field	Description
View		<p>To view a log from the LSM, select Events > Logs. Then, click the name of the desired log.</p> <p>To customize the display, specify the desired value in the Records per page field.</p> <p>To page through log entries, use the Navigation functions in the upper and lower left corners:</p> <ul style="list-style-type: none"> << Go to first page < Go to previous page > Go to next page >> Go to last page
Download		<p>Click the Download icon to download an electronic copy of the log or report. When you click the icon, the Download Log page displays to specify filter criteria for the log entries to be included in the downloaded log.</p> <p>When you download some logs, the downloaded log file contains additional information that is not displayed in the LSM interface. For details, see Appendix C, “Log Formats”</p>
Search		Click the Search icon to search for an entry in the log or report. The Logs page displays a search page according to the selected log or report.
Reset		Use the Reset icon to clear a log of all current entries. The log will then begin compiling new information.

For additional details, refer to the following topics:

- [“Viewing Logs” on page 107](#)
- [“Downloading a Log” on page 107](#)
- [“Searching a Log” on page 109](#)
- [“Resetting a log” on page 108](#)
- [“Searching a Log” on page 109](#)

Viewing Logs

Logs can be viewed from the Events menu.

View a log file

STEP 1 From the LSM **Events** menu, click the name of the log you want to view.

STEP 2 Click the desired log.

The LSM updates to display the log page for the selected item.

For details on managing the logs from the log page, see [“Managing Logs” on page 106](#).

Downloading a Log

To save log data, use the download function.

The X family device maintains two files for each log: a historical log file and a current log file. When the current log file reaches the default size (4MB), the log is de-activated and saved as the historical file, and a new log file is started as the current log. If a historical file already exists, that file is deleted.

In the LSM, the log view displays both current and historical log entries. When you download a log file, you have the option to download all the entries, or only the entries in the current log file.

The download function provides the following options:

- Download the entire log, or selected entries based on the following user-specified filter criteria:
 - **All** — Downloads all entries in the current and historical log files
 - **Current** — Downloads only the entries in the current log file
 - **Time Range** — Specifies the dates and times [optional] for compiling entries.
 - **ID Range** — Range of ID numbers for logged entries.
- View the log in a web browser
- Export the downloaded information to a comma-delimited text file (csv).



Note Downloaded logs provided more detailed information on each event than what is displayed in the LSM interface. For more information, see [Appendix C, “Log Formats”](#).

In the downloaded log, file entries are in a tab-delimited format with a line feed character terminating each line. Use WordPad or a spreadsheet application to view downloaded log files on a Windows workstation.

Download a Log

STEP 1 On the log page in the **Log Functions** section, click the Download icon.



Note If the log is empty, the download link will be disabled, or grayed out.

STEP 2 Verify that the **Log Type** dropdown list box has the correct log selected.

STEP 3 In the **Log Entry** section, specify the criteria for the log entries to be included in the downloaded file:

- Select **All** to download all entries.

OR

- Select **Current** to download all current entries.

OR

- Enter a **Time Range**, including the date [required] in YYYY-MM-DD format and time [optional] in HH:MM:SS format.

OR

- Enter an **ID Range** for entries in the **From** and **To** fields.

STEP 4 In the **Options** section, select one or both boxes for file format options: **Comma delimited format (csv)** or **Open in Internet Explorer**.

STEP 5 Click **Download**.

Resetting a log

When you reset a log, the LSM starts a new log file beginning with the current date and time based on the system time. All previous information is permanently deleted. For record keeping, you may want to download the log before performing a reset. (For details, see [“Downloading a Log” on page 107](#)).

Reset a Log

STEP 1 On a the log page in the Log Functions section, click Reset.

STEP 2 A confirmation message displays, prompting if you want to reset the log.

STEP 3 Click **OK**.

Searching a Log

Some logs provide a search function to help locate specific entries. This feature is available on the Alert, Audit, IPS Block Log, Firewall Block Log. To locate an entry within a log file, use the Search function available on each log page. You can search for entries by specifying one or more of the following criteria:

- **Date Range** — Search all log entries or specify a date range. You can also enter a time range.
- **Severity** — The severity includes low, minor, major, and critical events. You can select any severity you want to search.
- **Filter Name** — You can search for logged entries based on the filter that triggered them.
- **Protocol** — You can search by name of the protocol that the action affects.
- **Source Address** — You can search for a source address of the triggering traffic.
- **Destination Address** — You can search for a destination address of the triggering traffic.

Search a Log

- STEP 1** Open the log view. Then, in the Log Functions section, click [Search](#).
- STEP 2** On the Search System Log page, specify the search criteria For the **Log Entry Time**, choose a search option:
- Choose **All** to search all log entries.
- OR**
- Enter a date range for log entries. You can enter a date and time for the range, using the formats Year-Month-Date (YYYY-MM-DD) [required] and hours minutes seconds (HH:MM:SS) [optional].
- STEP 3** Check the box next to each **Severity** of the alerts you wish to retrieve [optional].
- STEP 4** Enter the name of the **Filter Name** whose alerts you would like to find [optional].
- STEP 5** Enter the name of the **Protocol** whose alerts you would like to find [optional].
- STEP 6** Enter the **Source Address** for alerts you would like to find. [optional].
- STEP 7** Enter the **Destination Address** for the alerts you would like to find [optional].
- STEP 8** Choose the **# of Results to Display** from the drop-down box [optional].
- STEP 9** Click **Search**.



TIP In Step 4 through Step 7, you can enter the first part of the item you want to search for. For example you can enter the first few letters or numbers in a filter name, or the first few numbers of an IP address.

Managed Streams

The Managed Streams menu pages provide options to review and manage traffic streams that have been blocked, rate-limited, or quarantined by IPS policies. These events are captured by the Threat Suppression Engine (TSE), which uses a blend of ASICs and network processors to detect threats and anomalies in network traffic.

The traffic streams include the following:

- **Blocked streams**— Traffic streams detected and blocked based on filters configured with a Block action set.
- **Rate-Limited streams** — Traffic streams detected and rate limited based on filters configured with a Rate-Limit action set.
- **Quarantined streams** — Traffic streams detected and blocked based on filters configured with a Quarantine action set, or quarantined manually.

For details, see the following topics:

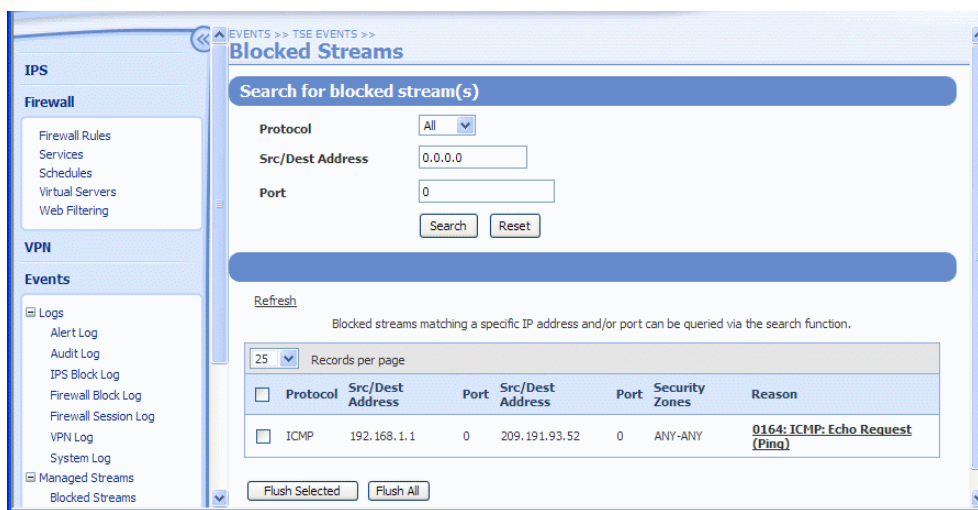
- [“Blocked Streams” on page 110](#)
- [“Rate Limited Streams” on page 112](#)
- [“Quarantined Addresses” on page 113](#)
- [“Action Sets” on page 44](#)

Blocked Streams

When traffic triggers an IPS filter that has been configured with a Block or Block+Notify action, traffic from the source IP address and port is blocked and an entry is added to the Blocked Streams page, based on the contact configuration in the action set. From the Blocked Streams page, you can:

- View and search for information on blocked streams
- Manually terminate all or selected blocked stream connections

Figure 5–1: Blocked Streams Page



The Blocked Log Entries table displays up to 50 entries. Entries are added when the block event occurs. Entries are automatically removed when the connection times out based on the **Connection Table timeout** setting configured from the IPS > IPS Preferences page. The default timeout settings is 1800 seconds (30 minutes). You can manually remove an entry by terminating the connection using the **Flush** functions.

For each blocked traffic stream, the Blocked Streams page provides the following information:

Table 5–9: Blocked Streams Table

Field	Description
Protocol	Protocol used by the blocked connection
Src/Dest Address	Source or destination IP address of the connection.
Port	Port of the connection
Src/Dest Address	Source or destination IP address of the connection
Port	Port of the connection
Security Zones	The security zones where traffic was blocked or rate-limited.
Reason	The filter link that details why the traffic connection stream was blocked. Click the link to display and manage the filter.

Search Blocked Streams

STEP 1 From the LSM menu, select **Events > Managed Streams > Blocked Streams**.

STEP 2 Enter search criteria for any of the following:

- Protocol — The protocol for the connection: All, TCP, UDP, ICMP
- Source or Destination Address — The traffic source or destination IP address
- Source or Destination Port — The traffic source or destination IP port

Entering “0” or “0.0.0.0” in the fields you do not want to specify allows you to search on any of the 4 fields (combination or single). This value acts as the value “any”.

STEP 3 Click **Search**.

To reset the search, click **Reset**.

Flush Blocked Streams

You can manually drop the connection for all or selected streams using the Flush functions available on the Blocked Streams page. A connection is automatically dropped when the connection table timeout period expires.

STEP 1 From the LSM menu, select **Events > Managed Streams > Blocked Streams**.

STEP 2 To drop all the connections, scroll to the bottom of the Blocked Streams page. Then, click **Flush All**.

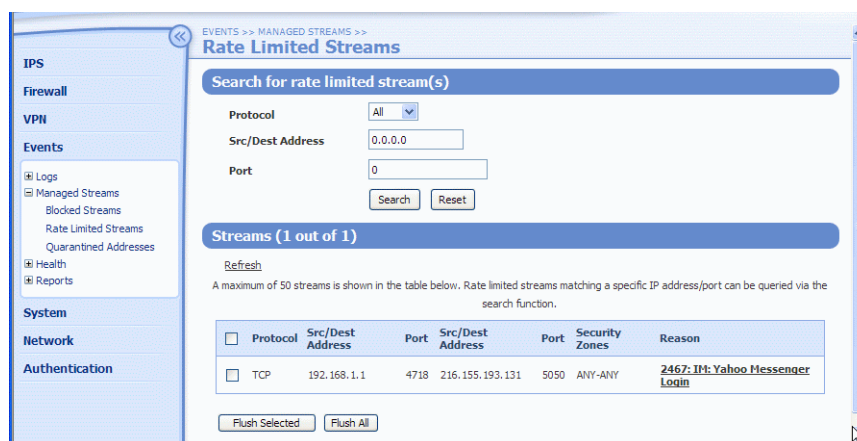
To drop selected connections, use the check box next to an entry to select it. Then, scroll to the bottom of the page and click **Flush**.

Rate Limited Streams

When traffic triggers an IPS filter configured with a Rate Limit action set, traffic from the source IP and port is limited based on the rate limit settings in the action set. Traffic from the source IP address and port to the destination IP address and port remains rate-limited until the connection timeout period expires, or until the connection is manually terminated from the LSM.

The following figure shows the Rate Limited Streams page.

Figure 5–2: Rate Limited Streams Page



From the Rate Limited Streams page, you can:

- View and search for information on rate-limited streams
- Manually terminate all or selected rate-limited stream connections

For details on performing these tasks, see [“Search rate-limited streams” on page 113](#) and [“Flush rate-limited streams” on page 113](#).

The Rate Limited Streams table displays up to 50 entries. Entries are added when the rate-limit event occurs. Entries are automatically removed when the connection times out based on the **Connection Table timeout** setting configured from the IPS Preferences page (**IPS > IPS Preferences**). The default timeout setting is 1800 seconds (30 minutes). You can manually remove an entry by terminating the connection using the **Flush** functions.

For each rate-limited stream, the **Rate Limited Streams** table provides the following information:

Table 5–10: Rate Limited Streams Table

Column	Definition
Protocol	Protocol used by the blocked connection
Src/Dest Address	Source or destination IP address of the connection
Port	Port of the connection
Src/Dest Address	Source or destination IP address of the connection
Port	Port of the connection

Table 5-10: Rate Limited Streams Table (Continued)

Column	Definition
Security Zone (pair)	The Security Zone pair where the stream is rate limited (LAN - WAN, for example)
Reason	The filter link that details why the traffic connection stream was blocked. Click the link to display and manage the filter.

Search rate-limited streams

STEP 1 From the LSM menu, select **Events > Managed Streams > Rate Limited Streams**.

STEP 2 Enter search criteria for any of the following:

- Protocol — The protocol for the connection: All, TCP, UDP, ICMP
- Source or Destination Address — The traffic source or destination IP address
- Source or Destination Port — The traffic source or destination IP port

Entering “0” or “0.0.0.0” in the fields you do not want to specify allows you to search on any of the four fields (combination or single).

STEP 3 Click **Search**.

To reset the search, click **Reset**.

Flush rate-limited streams

You can manually drop the connection for all or selected streams using the Flush functions available on the Rate Limited Streams page. A connection is automatically dropped when the connection table timeout period expires.

STEP 1 From the LSM menu, select **Events > Managed Streams > Rate Limited Streams**.

STEP 2 To drop all the connections, scroll to the bottom of the Rate Limited page. Then, click **Flush All**.

To drop selected connections, use the check box next to an entry to select it. Then, scroll to the bottom of the page and click **Flush**.

Quarantined Addresses

When traffic triggers an IPS filter configured with a Quarantine action set, the IP address of the host is quarantined. The host remains in quarantine with limited or no network access based on the settings configured in the quarantine action set, or until the address is manually removed from quarantine via the Quarantined Addresses page in the LSM, or until the global quarantine timeout (**IPS > Preferences**) expires.

Entries are added to the Quarantined Addresses page when the quarantine event occurs. Entries are automatically removed when the address is removed from quarantine either automatically based on the quarantine threshold settings for the action set, manually using the **Remove** function, or when the quarantine timeout expires.

From the Quarantined Addresses page, you can:

- View and search for information on quarantined addresses
- Force an address into quarantine
- Remove all or selected addresses from quarantine

The following figure shows the Quarantine Addresses page:

Figure 5–3: Quarantined Addresses Page

For each quarantined address, the Quarantined Addresses page provides the following information:

Table 5–11: Quarantined Address Table

Column	Description
IP address	The IP address of the host in quarantine.
Reason	Identifies the IPS filter that triggered the quarantine. Click the filter link to display and manage the filter.

For additional details, see the following sections:

- [“Configure a Quarantine Action Set” on page 51](#)
- [“Search for quarantined addresses” on page 114](#)
- [“Force IP address into quarantine” on page 115](#)
- [“Remove IP addresses from Quarantine” on page 115](#)

Search for quarantined addresses

STEP 1 From the LSM menu, select **Events > Managed Streams > Quarantined Addresses**

STEP 2 Enter a valid IP address for the quarantined host.

To view all quarantined addresses, the IP Address field must contain the value 0.0.0.0. This value is equivalent to the value *any*.

STEP 3 Click **Search**.

The Quarantined Addresses table updates with addresses matching the search criteria.

To reset the search field and update the Quarantined Addresses table to display all entries, click **Reset**.

Force IP address into quarantine

To manually quarantine a host, you must first configure a Quarantine action set which determines the behavior when the host attempts to access the network. As soon as you force the quarantine, the host immediately has limited or no network access based on the Quarantine action set configuration. For example, if the action set is configured to display a quarantine page, any requests from the host are redirected to the specified page.

STEP 1 From the LSM menu, select **Events > Managed Streams > Quarantined Addresses**.**STEP 2** Click **Quarantine**.

The Quarantined Addresses table updates to display the IP address of the quarantined host. Use the **Remove** function to manually remove the host from quarantine.

Remove IP addresses from Quarantine

You can manually remove all or selected IP addresses using the Remove functions available on the Quarantined Addresses page. An address may be automatically removed based on the quarantine threshold configuration for the Quarantine action set.

STEP 1 From the LSM menu, select **Events > Managed Streams > Quarantined Addresses**.**STEP 2** To remove all connections from quarantine, scroll to the bottom of the page. Then, click **Remove All**.

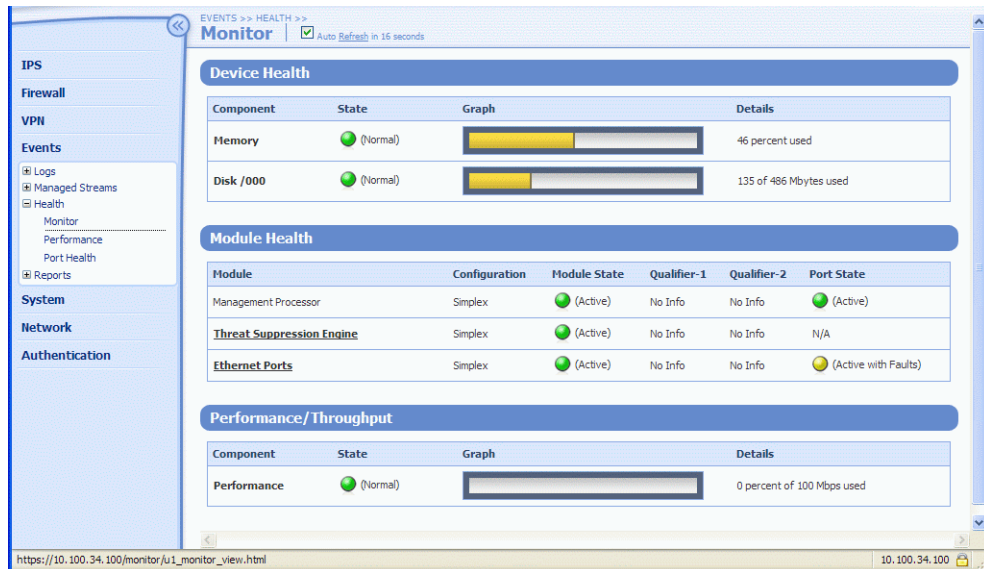
To remove selected addresses, use the check box next to an entry to select it. Then, scroll to the bottom of the page and click **Remove**.

Health

The Health menu pages show the current status and network performance of the X family device. From the Monitor page you can review:

- Device health indicated by memory and disk usage statistics
- Module health including the Threat Suppression Engine and Ethernet ports
- Performance/Throughput

Figure 5–4: Monitor Page



To access the Monitor page, select **Events > Health > Monitor**, or click **Health** on the System Summary page.

For details on each type of Health information, see the following:

- [“Device Health” on page 117](#)
- [“Module Health” on page 118](#)
- [“Performance/Throughput” on page 120](#)
- [“Port Health” on page 120](#)

Device Health

The Device Health section of the Monitor page displays the current status of a variety of chassis components, including power modules, fans, temperature, and memory and disk space usage.

Table 5-12: Device Health

Column	Description
Component	The component or resource being monitored. These components include the following: <ul style="list-style-type: none"> • Memory - the amount of memory used • Disk/000 - the amount of disk space available
State	The current operating status of the component or resource being monitored. The state can be one of the following: <ul style="list-style-type: none"> • Normal — usage is at normal levels • Major — usage has reached the major threshold setting specified for the device • Critical — usage has reach the critical threshold setting specified for the device To set the thresholds that trigger the Major and Critical states for memory and disk usage, select System > Configuration > Thresholds .
Graph	A representation of the current usage level of the component or resource being monitored.
Details	The units being measured in the graph. For example, for the memory component, this field index the percentage of total memory being used.

Memory and Disk Usage

The Memory Usage statistic displays usage averaged over the last refresh period. These values fluctuate fairly frequently. If Memory Usage percentages seem consistently high, check your log for Memory Fault messages.



Note If device health is consistently showing yellow or red warnings about Disk or Memory Usage, but the log does not show any hardware fault messages, your usage is spiking, but is not remaining consistently high.

If Memory Usage percentages are consistently high, you may need to adjust some IPS filter or Firewall Rule settings. Filters that require notification actions require more resources than filters that do not

require notification, but this difference only comes into play when network traffic matches or nearly matches these filters. Firewall rules with logging enabled also consume more memory.



TIP To reduce memory and disk usage, use the LSM to make the following filter adjustments:

- Reduce the number of IPS filters that use alerts
- Reduce usage of packet trace and e-mail notification on action sets
- Increase aggregation periods for action sets that include alerts
- Use more global filters and fewer filter overrides
- Deactivate filters that do not apply to your network (for example: IIS filters are not relevant if you only have Apache servers)
- Reset logs from the System Summary page or use the CLI **clear log** command. The clear log command will clear all log entries from all log files. For record keeping, you may want to download existing log files before resetting a log, or configure a remote syslog server to offload the logs.
- Delete previously installed TOS version images from the System Update page.
- Reduce the number of Firewall rules with logging enabled.
- Reduce the inactivity timeout on Firewall rules. This allows the firewall to discard inactive sessions more quickly.

Module Health

The Module Health section of the Monitor page displays the current status of the module that are inside the chassis of the device. The following information is provided.

Table 5-13: Module Health

Column	Description
Module	<p>A brief description of the type of module. Possible values:</p> <ul style="list-style-type: none"> • Management Processor — The central processing and control system for the device. • Threat Suppression Engine — The TSE (the IPS engine) provides full threat detection and suppression. Receives data from the Ethernet ports, performs deep packet inspection on the data, and permits or blocks the data based on configuration of Security Profiles and traffic threshold policy. When you click the link, it displays the IPS Preferences page. See “Configure Threat Suppression Engine (TSE)” on page 58. • Ethernet Ports — The Ethernet ports on the X family device. When you click the link, it displays the Port Health page with detailed information on each port. See “Port Health” on page 120.
Configuration	<ul style="list-style-type: none"> • A one-word description of the configuration of the module. Possible values: • Simplex — A communications channel that can carry a signal in one direction • Duplex — A communications channel that can carry signals in both directions

Table 5-13: Module Health

Column	Description
Module State	<p>A description of the current operation state of the module. Possible values:</p> <ul style="list-style-type: none"> • Active — The module is active without errors • Active with Faults — The module is active but has errors • Stand-by — The module is waiting for traffic or usage in a stand-by mode • Out-of-service — The module is not working or disabled • Diagnostic — The module is running a diagnostic
Qualifier-1	A description of any reasons for an other-than-active state of the module
Qualifier-2	Additional description of any reasons for an other-than-active state of the module
Port State	<p>A description of the current port state. Possible values:</p> <ul style="list-style-type: none"> • Active — The port is active normally without errors • Active with Faults — The port is active with errors • Not Initialized — The port is not out of service but the device has not initialized the hardware • Stand-by — The port is waiting for traffic or usage in a stand-by mode • Out-of-service — The port is not working or disabled due to errors • Diagnostic — The port is running a system check diagnostic applications or being repaired

Performance/Throughput

To view the current throughput performance of the device, select **Events > Monitor > Performance**. If the device is experiencing performance problems, the following information is provided.

Table 5-14: Performance/Throughput

Column	Description
Component	The component or resource being monitored. On this page, the component is device throughput performance
State	The current operating status of the component or resource being monitored. The state can be one of the following: <ul style="list-style-type: none"> • Normal — The device is active without errors • Major — The device is active but has errors • Critical — The device is waiting for traffic or usage in a stand-by mode • Out-of-service — The device is not working or disabled • Diagnostic — The device is running a diagnostic
Graph	A representation of the current status of the component or resource being monitored
Details	Percentage of throughput used.
System Performance Messages	This table provides information about current system performance. If the device is experiencing problems, the table displays messages indicating the cause of the problem along with suggested remedies.

Port Health

To view Port Health information for each Ethernet port on the device, select **Events > Health > Port**. The following information is provided:

Table 5-15: Port Health

Column	Description
Port	The number of the port on the device
Speed	The speed of the port
Duplex	Indicates if the port is set to full or half for duplex
State	A description of the current operation state of the module. Possible values: <ul style="list-style-type: none"> • Active — The module is active without errors • Active with Faults — The module is active but has errors • Stand-by — The module is waiting for traffic or usage in a stand-by mode • Out-of-service — The module is not working or disabled • Diagnostic — The module is running a diagnostic

Table 5-15: Port Health (Continued)

Column	Description
Qual-1	A description of any reasons for an other-than-active state of the module
Qual-2	Additional description of any reasons for an other-than-active state of the module
Media	The type of media of the port, such as copper or fiber
Type	The type of the port, such as Ethernet

Reports

The **Reports** menu provides access to detailed information about the LSM system alert and traffic activity. Data for each report is gathered in real time. You can use the **Refresh** option on each report page to get the most current report information.

The following Reports menu options are available:

- **Attacks** — displays data on traffic that has been filtered by the device based on the IPS filter and firewall rule configuration in a Security Profile.
- **Rate Limits** — Displays a bar graph showing the percentage of rate limit bandwidth used for each action set configured with a rate limit.
- **Traffic** — Displays traffic flow data categorized by transmission type, protocol, frame size, and port.
- **Traffic Thresholds** — Displays a bar graph of traffic that has triggered a traffic threshold filter. The report graphs the amount of incoming traffic as a function of time
- **Quarantine** — Displays a bar graph showing quarantine activity as a function of time.
- **Adaptive Filter Events** — Displays the global Adaptive Filter settings and a list of the 10 most recent filters impacted by adaptive filtering. You can also edit the Adaptive Filter settings from this report page.
- **Firewall** — Displays a bar graph showing the hit counts for each firewall rule as a percentage of total traffic based on firewall sessions.

For additional information, see the following:

- [“View a Report” on page 121](#)
- [“Attack Reports” on page 122](#)
- [“Rate Limit Reports” on page 123](#)
- [“Traffic Reports” on page 123](#)
- [“Traffic Threshold Report” on page 125](#)
- [“Quarantine Report” on page 125](#)
- [“Configure Adaptive Filter Events Report” on page 125](#)
- [“Firewall Reports” on page 126](#)

View a Report

STEP 1 From the Reports menu (**Events > Reports**), click the desired Report menu option.

STEP 2 On the selected Reports page, click any available view options to update the report data.

STEP 3 To update the report data, use the **Refresh** option. On some reports, an **Animate Charts** option is available to update the data in real time.

Attack Reports

The Attack Reports page allows you to view data on traffic that has been filtered by the device based on the IPS filter and firewall rule configuration. Firewall rules display as filter ids in the 7400 to 7410 range. For example, filter ID 7400 is the default DENY ANY ANY rule that implicitly added to the end of the Firewall Rule table.

Traffic data is reported based on the view options you select:

- **Top Ten Filters** — displays a bar graph of the top 10 attack filters which includes a packet counter, and the percentage of total traffic affected by the filter.
- **Severity** — displays the number of attacks categorized as Low, Minor, Major, and Critical. The graph also shows the percentage of total traffic for each severity level. The severity levels are assigned by the TippingPoint Digital Vaccine team and are included as part of the filter definition.
- **Action** — displays the actions taken on filtered traffic: traffic can be dropped (Invalid), blocked, or permitted. The report includes the number of packets processed by each action and the percentage of total traffic the number represents.
- **Protocol** — displays attack traffic categorized by protocol. The report includes the number of filtered packets for each protocol and the percentage of total traffic the number represents. Protocols include: ICMP, UDP, TCP, AND IP-Other
- **By Port: All** — displays amount of all attack traffic reported by the Security Zone where the traffic was filtered, number of packets is reported as a percentage of total traffic
- **By Port: Permit** — displays amount of attack traffic permitted reported by Security Zone. Number of packets is reported as a percentage of total traffic.
- **By Port: Block** — displays amount of attack traffic blocked reported by Security Zone. Number of packets is reported as a percentage of total traffic.

Update report data

To update the traffic statistics in real time information, select the **Animate Charts** option. If this option is not selected, click the **Refresh Data** link to view the most current information.



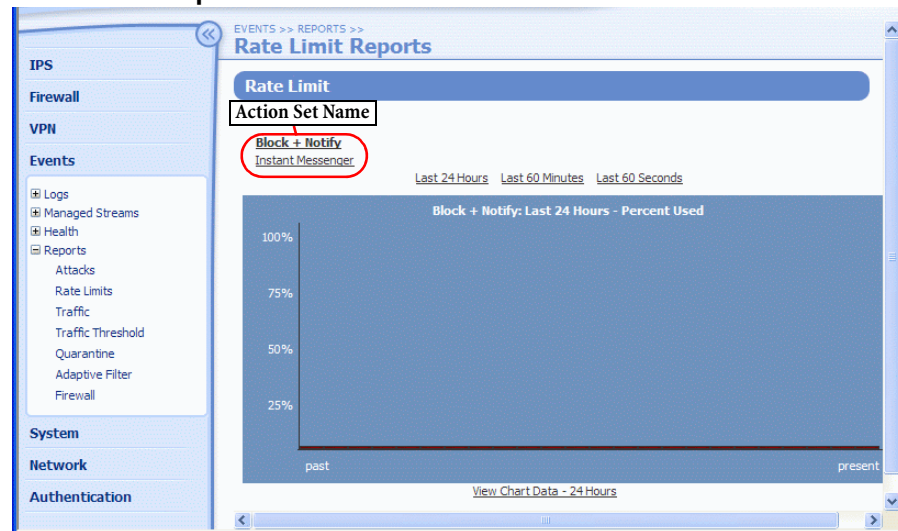
Note Additional information on attack filter events is available in the LSM logs. For details, see [“Logs” on page 98](#).

Rate Limit Reports

In the LSM, you can configure a rate limit action set to define the maximum amount of bandwidth available for traffic matching IPS filters that have a rate limit action set assigned. If two or more IPS filters use the same rate limit action set, then all packets matching these filters share the bandwidth. For each rate limit action set, the Rate Limit Reports page allows you to view the percentage of bandwidth consumed by rate-limited traffic graphed as a function of time.

The following figure shows the Rate Limit Reports page:

Figure 5–5: Rate Limit Reports



Data is reported based on the view options you select in the Rate Limit Reports page:

- **Rate Limit Action Set Name** — the list of available rate limit action sets is provided at the top of the rate limit table. To view the percentage of rate-limited bandwidth used for an action set, click on the action set name to update the report.
- **Reporting time interval** — select the time interval for the reporting period: **Last 24 hours**, **Last 60 Minutes**, **Last 60 seconds**.



Note The Rate Limit report is only available if an Action Set has been configured with the Rate Limit action.

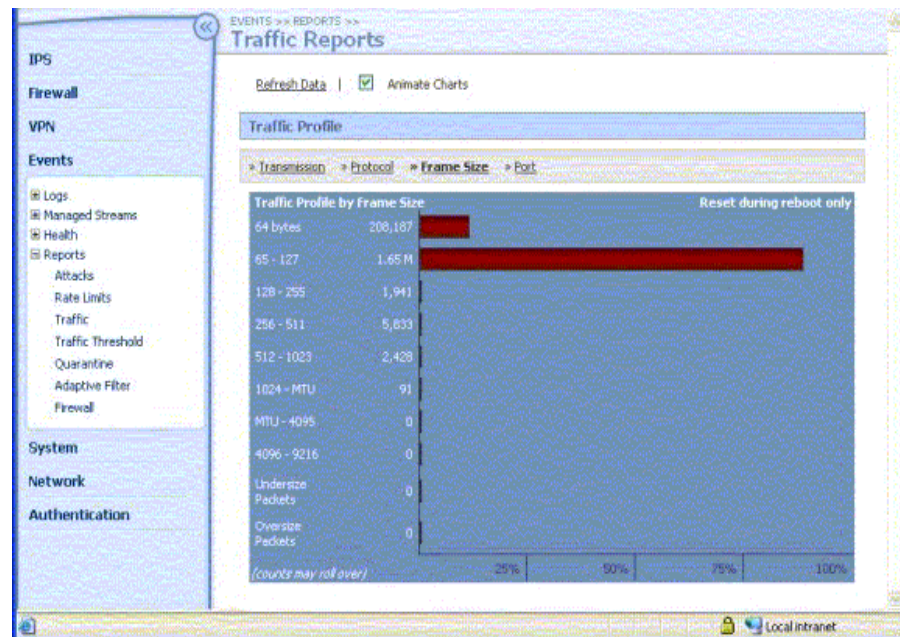
For additional information on rate limit action sets, see [“Action Sets” on page 44](#). For details on rate-limited traffic streams, see [“Rate Limited Streams” on page 112](#).

Traffic Reports

The traffic report provides profile data on the packets flowing through the device (permitted packets only).

The following figure shows the Traffic Profile Reports page..

Figure 5-6: Traffic Profile Reports - by Protocol



Traffic data is reported based on the view option you select on the Traffic Reports page:

- **Transmission Types** — graphs the number of packets transmitted for each of the following transmission categories: Unicast, Broadcast, MultiCast, MAC control, FCS Errors, Align Errors
- **Protocol** — graphs the number of packets transmitted by ICMP, UDP, TCP, IP-other, ARP, and Ethernet-Other
- **Frame size** — Traffic profile by framesize, by specified byte ranges
- **By Port** — Traffic profile by port, includes all security zones/ports

Update report data

To update the traffic statistics in real time information, select the **Animate Charts** option. If this option is not selected, click the **Refresh Data** link to view the most current information.

Traffic Threshold Report

In the LSM, traffic threshold filters track statistical changes in network traffic patterns. You can specify the amount of traffic that triggers a Traffic Threshold filter from the Traffic Threshold Reports page. The units used in the report (packets/hour, bytes/minute, connections/second, etc.) is determined by the units configured in the Traffic Threshold filter.



Note The Traffic Threshold report is only available if an IPS Traffic Threshold filter has been configured for the device.

Traffic data is reported based on the viewing options you select on the Traffic Threshold Reports page:

- **Traffic Threshold filter name** — in the dropdown list under the Traffic Thresholds table heading, select the filter name to generate the traffic data for that filter.
- **Reporting time interval** — click the time interval for the reporting period: **Last 35 Days**, **Last 24 hours**, **Last 60 Minutes**, **Last 60 seconds**.

For additional information, see the [“Traffic Threshold Filters” on page 38](#).

Quarantine Report

In the LSM, you can configure a filter with a quarantine action set. When a host computer triggers the filter, the host is quarantined according to the settings configured in the action set. You can monitor quarantine activity from the Quarantine Reports page.

Quarantine data is reported based on the viewing options you select on the Quarantine Reports page:

- **Total Hosts** — displays the total number of quarantined hosts as a function of time.
- **Packets Blocked** — displays the total number of packets blocked as a function of time.
- **Src Pages** — displays the number of LSM quarantine pages served to quarantined hosts as a function of time. The quarantine source pages are generated based on the configuration specified in the Quarantine action set.
- **Redirect Pages** — displays the number of times hosts have been redirected as a result of a quarantine action as a function of time.
- **Reporting time interval** — click the time interval for the reporting period: **Days** (last 35), **Hours** (last 24), **Minutes** (last 60), **Seconds** (last 60).



Note More detailed information on quarantined hosts is available from the Quarantined Addresses page. For details, see [“Quarantined Addresses” on page 113](#).

Configure Adaptive Filter Events Report

From the Configure Adaptive Filter Events Report page, you can:

- review and modify the global Adaptive Filter configuration
- view a list of the 10 most recent filters managed by adaptive filtering
- disable adaptive filter settings for an individual filter.

The Configure Adaptive Filter Events report page provides the following information:

Table 5-16: TSE Adaptive Filter Configuration Details

Column	Definition
Settings	The Settings table allows you to change the global system configuration for the Adaptive Filter function. For details, see “Adaptive Filter Configuration” on page 60 .
Ten Most Recent: Table that displays the ten most recent filters managed by adaptive filtering.	
Filter Name	The linked name of the filter being managed by the Adaptive Filter function. To disable Adaptive Filter Configuration for a filter, click the linked name. On the Edit Filter page, select the Do not apply adaptive configuration settings to this filter. Then, click the Apply button to save the setting.
Filter State	Indicates the current state of the filter. <ul style="list-style-type: none"> Enabled — Displays Enabled if the filter is enabled and running Disabled — Displays an empty value if the filter is disabled. To enable, edit the filter.
Adaptive Filter State	Indicates the adaptive state of the filter. If it displays Enabled , the filter is being managed by the Adaptive Filter configuration. If the Adaptive Filter configuration is set to Auto, the filter is automatically disabled. If the configuration is set to Manual, a message is generated in the system log, but the filter is not been disabled.
Functions	Icon representing functions to perform. These options may include resetting the filter and saving the packet trace.

For additional information on the Adaptive Filters, see [“Adaptive Filter Configuration” on page 60](#).

Disable Adaptive Filter settings for a filter

STEP 1 From the LSM menu, select **Events > Reports > Adaptive Filter**.

STEP 2 In the **Ten Most Recent** table, click the **Filter Name**.

STEP 3 On the Edit Filter page in the **Adaptive Filter Configuration State** table, click **Do not apply adaptive configuration settings to this filter**.

STEP 4 Click **Apply**.

After the setting is changed, the filter can no longer be managed by the Adaptive Filter function.

Firewall Reports

The Firewall Reports page provides links to data about the network as seen by the firewall (that is, traffic crossing security zones). The report timespan is the preceding 24 hours, or since the last reboot,

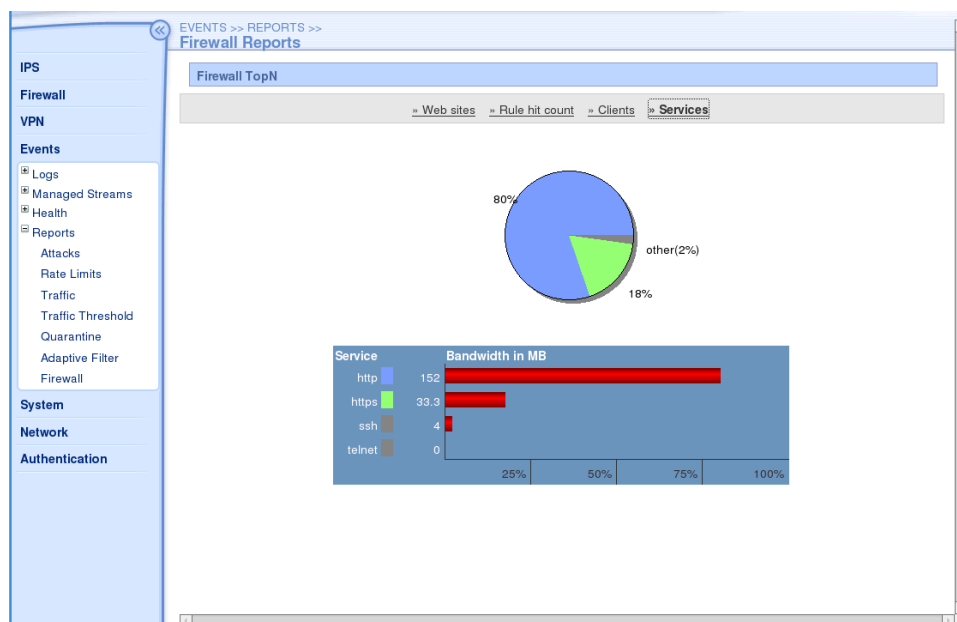
whichever is more recent. Data is added when the firewall session is closed; therefore, a large file transfer in progress, for example, will not be tabulated until after it finishes.

Data is presented as one of the following graphs:

- **Top Web sites** — The 25 most visited external Web sites by bandwidth. You must create a firewall rule to match with the “web-filter” action between zones that you wish to monitor. You do not need to enable either of the web filtering options (manual-filter or filter-service). Only connections to or from TCP port 80 are displayed. The web site name is extracted from the HTTP request headers; for requests that do not provide a host name or only an IP address, the IP is displayed. Sites with multiple domains or that host images and other data on different Web servers appear as multiple entries.
- **Firewall rule hits** — The 25 most triggered firewall rules. The “hit count” is the number of firewall sessions that have matched that rule in the table. The top ten rules are assigned colors. Unlike the other tables, which are sorted by bandwidth, entries in this table are displayed in order of precedence; rules outside of the first ten are listed as “other” even if they have larger hit counts.
- **Top clients** — The 25 protocols generating the most traffic to and from internal IP addresses by bandwidth. An internal address is one which is on an internal security zone, that is, one that is part of any internal virtual interface. Generally the only IP addresses not considered internal are those reached via a route out of the external virtual interface. Machines reached via PPTP, L2TP, and IPSec tunnels that terminate on an internal security zone are considered as internal addresses and can appear as clients.
- **Top services** — The 25 services consuming the most bandwidth. For TCP and UDP, the service name is determined from the IP protocol and destination port. Traffic for which there is no known service is shown as a generic name tcp(port), udp(port) or ip(protocol), such as “tcp(1234),” “udp(5001),” or “ip(100).” FTP connections are aggregated, but services such as p2p that use different port numbers appear as multiple entries and cannot be aggregated.

The following figure shows the Firewall Reports page.

Figure 5–7: Firewall Reports Page



6 Network

The Network section describes IP interfaces, security zones, DHCP functionality, routing, and IP address groups and explains how to enable, disable, and modify their various features. The network tools provided by the LSM are also described.

Overview

The Network menu pages in the LSM enable you to set up the X family device so that it can work within your network environment. The following menu options are available:

- **Network Ports** — manage port configuration (auto-negotiation and line speed), disable/enable or restart a port.
- **Security Zones** — create and manage security zones that logically segment your network by ports and VLANs so that you can apply firewall rules and IPS filters to traffic passing between sections.
- **IP interfaces** — manage and configure the internal and external IP interfaces the device uses to make the network connections for your environment. Each security zone must be associated with an IP interface.
- **IP address groups** — create and manage groups of IP address group by host, subnet, or address range. You can use these IP address group to simplify configuration of device features.
- **DNS** — configure the global DNS servers and search domains for the device, or choose to use the DNS configuration obtained from the WAN connection.
- **Default Gateway** — if you have configured the External Interface with a static IP address, use this option to manually configure the default IP address that the device uses to route packets when it has no other route to a given IP address.
- **Routing** — configure the static and dynamic routing for the device and enable/global options for unicast (RIP) and multicast routing (IGMP, and PIM-DM)
- **DHCP Server** — enable the device to act as a DHCP server and configure the server settings.
- **Tools** — access tools to lookup DNS names, find the physical interface/security zone that the device would use to reach a given location, capture traffic on the device for analysis, ping devices on the network, and trace the network hops traffic takes from the device to another device in the network.

For additional information, see the following topics:

- [“Configuration Overview” on page 130](#)
- [“Deployment Modes” on page 131](#)
- [“Network Port Configuration” on page 132](#)
- [“Security Zone Configuration” on page 135](#)
- [“IP Interfaces” on page 140](#)
- [“IP Address Groups” on page 153](#)
- [“DNS” on page 155](#)
- [“Default Gateway” on page 156](#)
- [“Routing” on page 157](#)
- [“DHCP Server” on page 167](#)
- [“Network Tools” on page 176](#)

Configuration Overview

The X family device has a default configuration so that the device can pass traffic in most network environments after it has been installed and configured using the Setup Wizard. However, you may need to customize the configuration for your network. The following provides a list of common configuration steps.

- STEP 1** Select the deployment mode: Full Transparent, Transparent DMZ - NAT Routed LAN, full routed/NAT deployment.
- STEP 2** Configure IP Address Groups to use when creating Security Zones and configuring the DHCP server (optional).
- STEP 3** Define IP Interfaces.
- STEP 4** If you configure the external IP interface to use a static IP address, define the default gateway.
- STEP 5** Create Security Zones.
- STEP 6** Configure Firewall Rules (see [“Firewall” on page 63](#)).
- STEP 7** Configure DNS servers.
- STEP 8** Define routing static, unicast, and multicast routing for your network.
- STEP 9** Configure the default gateway (or route).
- STEP 10** Configure DHCP Server (optional).

For additional information, see the following topics:

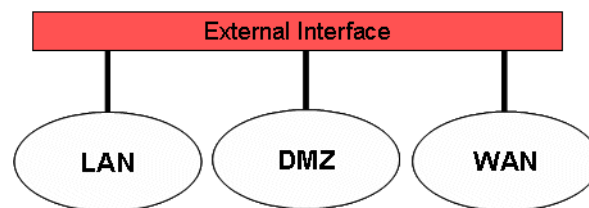
- [“Deployment Modes” on page 131](#)
- [“Network Port Configuration” on page 132](#)
- [“Security Zone Configuration” on page 135](#)
- [“IP Interfaces” on page 140](#)
- [“IP Address Groups” on page 153](#)
- [“DNS” on page 155](#)
- [“Default Gateway” on page 156](#)
- [“Routing” on page 157](#)
- [“DHCP Server” on page 167](#)
- [“Network Tools” on page 176](#)

Deployment Modes

The deployment mode you select determines how to configure the IP interfaces and routing on the device. You have the following ways to implement security zones, depending on your current network deployment:

- **Transparent** — In this mode, the device behaves like a layer 2 switch, except that you can still enforce security policy (firewall rules, web content filtering, IPS filtering, etc.) between security zones. All devices share the same IP address which means that you only have one IP interface for all security zones in the same transparent group. All security zones are in the same broadcast domain.

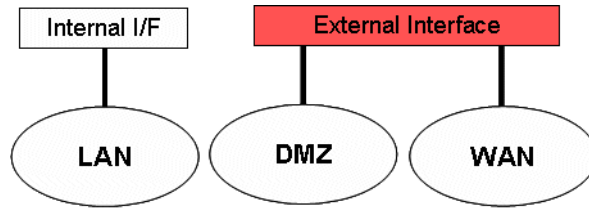
Figure 6–1: X Family Transparent Deployment Mode



- **Transparent DMZ - NAT/Routed LAN** — In this mode, the network is divided into multiple IP subnets. Each security zone has a unique IP interface so that the devices within each zone have a unique IP address space. For example, hosts in the LAN zone use a private (RFC 1918) IP address range, while hosts in the WAN and DMZ zones use another IP address range. Private IP addresses originating in the LAN zone and going to the WAN zone are mapped to one or more public IP addresses using NAT. The internal and external IP interfaces are configured with private and public

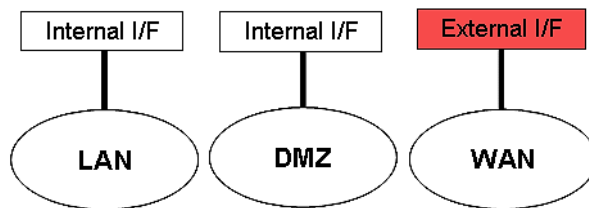
IP addresses, respectively. The LAN security zone is in one broadcast domain while the DMZ and WAN zones are in another.

Figure 6–2: X Family Transparent DMZ - NAT/Routed LAN Deployment Mode



- **Bridge** — In this mode, the device acts as a bridge to transparently connect security zones assigned to the same virtual interface. You do not have to configure IP routes to bridge traffic. When in bridge mode, the device learns MAC addresses on ports, and forwards traffic within the transparent virtual interface by destination MAC address to the appropriate port. If the address is unknown, the device forwards the packet to all ports. The device does not forward spanning tree packets. It still operates normally as a router and VPN terminator
- **Full routed/NAT** — In this mode, all security zones have unique IP addresses and addresses going to the WAN zone may be NAT'ed. Each security zone is in a separate broadcast domain.

Figure 6–3: X Family Full Routed/NAT Deployment Mode



For more detailed information and examples of deployment modes, refer to the *Concepts Guide*.

Network Port Configuration

Use the Network Port Configuration page to configure and manage the ports on the device. From this page you can complete the following tasks:

- Edit port configuration
- Restart a port
- Disable a port



TIP You can view the current status and port configuration from the Port Health page (**Events > Health > Port Health**).

The following figure shows the Port Configuration page:

Figure 6–4: Network: Configuration: Port Configuration Page

Port	Auto Negotiation	Line Speed	Duplex Setting	Media	Port Enabled	Restart
Port 1	<input checked="" type="checkbox"/>	100 Mbps	Full	Copper	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Port 2	<input checked="" type="checkbox"/>	100 Mbps	Full	Copper	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Port 3	<input checked="" type="checkbox"/>	100 Mbps	Full	Copper	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Port 4	<input checked="" type="checkbox"/>	100 Mbps	Full	Copper	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Port 5	<input checked="" type="checkbox"/>	100 Mbps	Full	Copper	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Port 6	<input checked="" type="checkbox"/>	100 Mbps	Full	Copper	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Apply

The Port Configuration page provides the following information:

Column	Description
Port	The port number on the device.
Auto Negotiation	Indicates whether the port auto-negotiates line speed based on the Line Speed setting. If Auto Negotiation is enabled, the device automatically selects the correct line speed and duplex setting based on the device port it is connected to. If Auto Negotiation is disabled, the port will negotiate between the available line speeds.
Line Speed	Indicates the line speed setting for the port is 10 or 100 Mbs.
Duplex Setting	Indicates whether the port is set to full, half, or duplex.
Media	Indicates whether the port is Copper or Fiber.
Port Enabled	Indicates whether the port is currently enabled or disabled.
Restart	If selected, the port is restarted when you click Apply .

Port Configuration Tasks

For additional information, see the following topics:

- [“Edit Port Configuration” on page 134](#)
- [“Disable a Port” on page 134](#)
- [“Restart a Port” on page 134](#)
- [“Correct a Port Link-Down Error” on page 134](#)

Edit Port Configuration

- STEP 1** From the LSM menu, select **Network > Configuration > Network Ports**.
- STEP 2** On the Port Configuration page, clear the **Auto Negotiation** checkbox for the port you want to configure.

The page updates to show configuration fields for Line Speed and Duplex Setting.
- STEP 3** Select the **Line Speed** setting from the drop-down menu.
- STEP 4** Select the **Duplex** setting: **Full** or **Half**.
- STEP 5** Check the **Restart** checkbox.
- STEP 6** Click **Apply** to save the configuration and restart the port.

Disable a Port

- STEP 1** From the LSM menu, select **Network > Configuration > Network Ports**.
- STEP 2** On the Port Configuration page, clear the **Port Enabled** checkbox.
- STEP 3** Check the **Restart** checkbox.
- STEP 4** Click **Apply** to save the configuration and restart the port.

Restart a Port

- STEP 1** From the LSM menu, select **Network > Configuration > Network Ports**.
- STEP 2** On the Port Configuration page, check the **Restart** checkbox.
- STEP 3** Click **Apply** to save the configuration and restart the port.

Troubleshoot Port Link-Down errors

If the X family device indicates that the ports are unable to establish link, check the connections on the device. If you use a copper-fiber translator (such as Netgear) and it is disconnected or loose, the device driver will attempt to re-initialize the port several times before timing out and placing the port in an Out-of-Service mode.

Netgear does not support auto-negotiation. When you remove the copper cable or the cable is loose, Netgear does not attempt to auto-negotiate with the device.

Correct a Port Link-Down Error

- STEP 1** From the LSM menu, select **Network > Configuration > Network Ports**.
- STEP 2** On the Port Configuration page, clear the **Auto Negotiation** checkbox for the port that is not working.
- STEP 3** Click the **Restart** checkbox. Then, click **Apply** to restart the port.

Security Zone Configuration

A security zone is a section of the network which is associated with a port or VLAN. If you need to control the traffic between devices, the devices must be in separate security zones. Using the LSM, you can add, edit, or delete security zones.

Security zones enable you to logically segment your networks so that the device can apply firewall rules and IPS filters to control the traffic passing between the zones. Typically, each Ethernet port and VPN tunnel on the device is associated with one security zone, unless you use VLANs. If you configure VLANs, then a port can be in more than one security zone. For further information on Security Zones, refer to the *Concepts Guide*.

Any traffic originating from or destined to devices in a zone will be directed through the device and policed by firewall policies, if the traffic passes through to another zone. However, traffic moving between devices within a given zone that you have defined (intra-zone traffic) will not be subject to firewalling or IPS filtering (for example, a user on the LAN zone, accessing the local LAN printer) and will not pass through the device.

Devices in your network that communicate freely and do not require restricted access between them should be placed in the same zone.

In the LSM, you can view and manage Security Zones from the Security Zone page (**Network > Configuration > Security Zones**). From this page you can complete the following tasks:

- View a summary of current configuration for all Security Zones
- Create a Security Zone
- Edit the configuration for a Security Zone
- Delete a Security Zone



The following figure shows the Security Zones page.

Figure 6–5: Network: Security Zones Page

Zone	Untagged Port(s)	VLAN ID	VLAN Port(s)	Bandwidth Mgmt	IP Addr Restrictions	Function(s)
LAN	1	1	-	No	-	
VPN		4	-	No	-	
WAN	4	3	-	No	-	
MGMT	2	5	-	No	-	
LAN3	3	6	-	No	-	

Create Security Zone

The Security Zones page provides the following information about each zone:

Column	Description
Zone	The name of the Security Zone. Initially, the device is configured with LAN, VPN and WAN default zones.
Untagged Port(s)	The ports on the device that have been assigned to each zone.
VLAN ID	Identifies the VLAN associated with the security zone (if applicable).
VLAN Port(s)	The physical ports that have been allocated to the VLAN (if applicable).
Bandwidth Management	Whether bandwidth rate limiting has been applied, and the access speeds in Kbps for outbound (upload) traffic and inbound (download) traffic across the device. Applying bandwidth limitation physically limits the rate of traffic flow.
IP Address Restrictions	The IP addresses for this security zone, either an IP Address Group , IP subnet or IP range .
Function(s)  	The functions available to manage the Security Zones: <ul style="list-style-type: none"> • Edit a Security Zone • Delete a Security Zone

For additional information, refer to the following topics:

- [“Create or Edit a Security Zone” on page 138](#)
- [“Configure a Security Zone” on page 139](#)

Creating, Editing and Configuring Security Zones

Each device is configured with the following default security zones.

Table 6–1: Default Security Zones

Preconfigured Zones	Ports
LAN	Port 1
WAN	Port 4
VPN	VLAN ID = 4

Although the device is preconfigured with default security zones, you can modify these or create your own security zones, with associated security policies and traffic shaping rules, based on your network environment and user requirements.

You can create and edit Security Zones from the Create/Edit Security Zone page.

Figure 6–6: Create/Edit Security Zone Page

The following table lists the Security Zone configuration parameters.

Table 6–2: Security Zone Configuration Parameters

Parameter	Description
Zone	Type a name for the security zone.
Ethernet Port(s)	Select one or more ports on the device to be assigned to the zone. If you select a port that is already assigned to another zone, the port will be reassigned to this zone.
Advanced Options	
Enable 802.1q VLAN Tagging	Option to enable VLAN tagging on the port(s) assigned to the Security Zone. Note With tagged ports, you can have as many security zones sharing a port as you require. Each zone must be associated with an IP interface.
VLAN Tagged Ports	If Enable 802.1q VLAN Tagging is enabled, select the physical ports that have been allocated to the VLAN.
VLAN ID	Identifies the VLAN associated with the security zone (if applicable).
MTU Size	Maximum transmission unit (MTU) size; enter a decimal number from 100 to 1500.

Table 6–2: Security Zone Configuration Parameters (Continued)

Parameter	Description
Bandwidth Management (rate limiting)	
Enable bandwidth rate limiting	<p>Select this option to specify bandwidth rate limiting for the access speed for outbound (upload) traffic and inbound (download) traffic across the device. Applying bandwidth limitation physically limits the rate of traffic flow. You can define separate limits for outbound and inbound traffic in <i>kbps</i>.</p> <p>Note Bandwidth Management is typically used to prevent packet queuing on a WAN device to provide lower end-to-end latency on latency sensitive traffic such as voice over IP.</p>
<p>Network Protection</p> <p>If you configure Network Protection options, verify that all IP hosts that use the zone are within the IP addresses specified. Hosts may include:</p> <ul style="list-style-type: none"> • directly attached hosts connected to the zone via the Ethernet ports associated with the zone • remote IP subnets connected via routers in the zone • IP Address pools specified for any PPTP or L2TP server where the VPNs terminate in the security zone. <p>This option is commonly used for transparent deployments to ensure that an IP address can appear in only one security zone.</p>	
IP Address Restrictions	<p>The IP addresses for this security zone, either an IP Address Group, IP subnet or IP range.</p> <p>Note If you do not specify any restriction, the device will automatically learn the IP addresses of clients in each Security Zone.</p>
Prevent Security Zone sending to VPN tunnels	Determines whether traffic is allowed from this security zone to an IPSec VPN tunnel.

Create or Edit a Security Zone

STEP 1 From the LSM menu, select **Network > Security Zones**.

STEP 2 On the Create Network Security Zone page, click **Create Security Zone** or click the **Edit** icon for the zone you want to modify.

STEP 3 On the Create/Edit Security Zone page, configure the zone as required.

For more information, refer to [“Configure a Security Zone” on page 139](#).

Configure a Security Zone

STEP 1 From the LSM menu, select **Network > Security Zones**.

STEP 2 Click **Create** (for a new security zone) or click the **Edit** icon for the zone you want to edit.

STEP 3 On the **Create/Edit Security Zone** type the **Security Zone Name** for the new zone.

You can only edit the Security Zone name when you are creating the zone.

STEP 4 Check the **Ethernet Ports** that you want to add to the zone.

If you select a port that is already assigned to another zone, the port will be reassigned to this zone.

You do not need to assign ports to a zone if you are using the zone solely for a VPN tunnel.



Note With tagged ports, you can have as many ports in a security zone as you require. However, you cannot configure firewall rules or IPS filters between ports in the same Security Zone.

STEP 5 If you want to enable VLAN tagging on the port(s) assigned to the Security Zone, check the **Enable 802.1q VLAN Tagging** option and enter a VLAN ID.



Note With tagged ports, you can have as many security zones sharing a port as you require. Each zone must be associated with an interface.

STEP 6 To set the maximum transmission unit (MTU) size, enter a decimal number from 100 to 1500 in the **MTU Size** field.

The default for Ethernet is 1500. Reducing the MTU ensures that packets sent over networks with smaller MTUs than Ethernet are not fragmented.

STEP 7 To apply **Bandwidth Management**, check **Enable bandwidth rate limiting**, and enter the required limits in Kbps (any decimal number from 1 to 100000) for **outbound traffic** and **inbound traffic** in the appropriate fields.

Bandwidth Management is typically used to prevent packet queuing on a WAN device to provide lower end-to-end latency on latency sensitive traffic such as voice over IP.

STEP 8 To restrict the IP addresses of clients in the Security Zone for additional security purposes, check **Restrict Security Zone to the following IP addresses**. Then, select one of the following.

- **IP Address Group** — select the name of the group from the drop-down list. (To configure IP Address Groups, navigate to **Network > Configuration > IP Address Groups**.)
- **IP Subnet** — type the IP network address and subnet mask.
- **IP Range** — type a range of IP addresses within the IP Interface subnet.

STEP 9 To prevent traffic going from this security zone to a VPN tunnel, check **Prevent Security Zone sending to VPN tunnels**.

STEP 10 Click **Create/Save** to save the configuration.

Click **Cancel** to discard the changes.

IP Interfaces

Configuration Overview

IP interfaces provide the X family device with the interfaces to make the network connections required for your environment. An IP interface is the Layer 3 configuration for the device, that is, the IP configuration for its set of security zones (and hence Ethernet ports within the security zones). Before configuring the IP interfaces for the device, you need to determine the deployment mode that best meets network requirements: transparent, transparent DMZ (NAT/Routed LAN), or full-routed/NAT. For a description of these deployment modes, see [“Deployment Modes” on page 131](#).

The device allows you to configure three types of IP interfaces: external, internal, and GRE. You can only configure one external interface on each device. For device maximum configurable values, see Appendix D, “Device Maximum Values”. Setting up the IP interfaces for a device is a three-step process:

- STEP 1** For each IP interface, configure the IP address information. An interface is required for every IP subnet that is directly connected to the device. For example, you need one for the Internet connection (external interface) and one for every directly connected network subnet (internal interfaces).
- STEP 2** For each IP interface, select the security zones that will use the configuration. Each security zone must be associated with an internal or external IP interface.
- STEP 3** If necessary, configure the interface to perform routing using the advanced configuration options.

For additional information, see the following topics:

- [“Managing IP Interfaces” on page 141](#)
- [“IP Addresses: Configuration Overview” on page 142](#)
- [“Configuring a GRE Tunnel” on page 148](#)
- [“Manage Security Zones for IP Interfaces” on page 149](#)
- [“Configuring Routing for IP Interfaces” on page 150](#)

Managing IP Interfaces

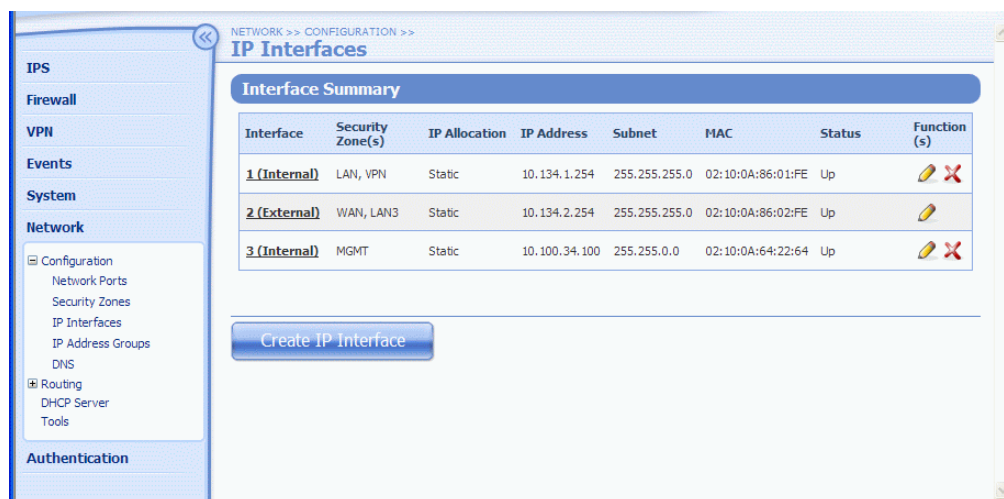
The IP Interfaces page (**Network > Configuration > IP Interfaces**), shows the IP interfaces that are currently configured on the device. From this page you can create, edit, or delete IP interfaces.



Note You can also configure IP interfaces using the device Setup Wizard. For details, see [“Setup Wizard” on page 242](#).



The following figure shows the IP Interfaces page:

Figure 6–7: IP Interfaces Page



The IP Interfaces page provides the following information about each interface:

Column	Description
Interface	The number of the interface, and the type of interface, either Internal or External . The maximum number of interfaces is 32
Security Zone(s)	The security zone assigned to the interface
IP Allocation	The allocation method and configuration for the interface
IP Address	The IP address of the interface

Column	Description
Subnet	The subnet mask for the interface
MAC	The MAC address for the interface. The device automatically assigns a unique MAC address for every virtual interface configured on the device.
Status	The status of the interface, either Up , or Down with brief details of why the interface is down
Function(s) The functions available to manage the IP Interfaces: <ul style="list-style-type: none">  • Delete an interface  • Edit the IP interface configuration 	

Manage IP Interfaces

STEP 1 From the LSM menu, select **Network > Configuration > Interfaces**.

STEP 2 On the IP Interfaces page, click the appropriate icon to **Edit** or **Delete** an interface.

To create an IP interface, click **Create IP Interface**. Then, on the Create IP Interfaces page, specify the configuration options.

For more information on configuring IP Interfaces, see [“IP Addresses: Configuration Overview” on page 142](#).

IP Addresses: Configuration Overview

For each IP interface required, select the IP address allocation method and configure the required parameters from the IP Interfaces Create or Edit page.

The following allocation methods are available based on whether you are configuring an internal or external interface:

- **Internal (LAN) Interfaces** —the only addressing method available on an internal IP interface is **Static IP Address**
- **External (WAN) Interface** — Typically, this is the interface that the device uses to connect to your Internet Service Provider (ISP). You can only configure one external IP interface on the device. Choose from the following allocation methods:
 - **Static IP Address** — select this if are using a public static IP address, or if your ISP has allocated you a public static IP address.
 - **DHCP** — select this if your ISP has told you to use DHCP, or you are connecting to a device that provides IP configuration using DHCP. DHCP is the default IP allocation method for the device external interface.
 - **PPTP client** — select this if your ISP is using PPTP to provide your IP configuration.
 - **L2TP client** — select this if your ISP is using L2TP to provide your IP configuration.
 - **PPPoE client** — select this if your ISP is using PPPoE to provide your IP configuration.

For details on configuring the IP address for each type of interface, see the following topics:

- [“Internal Interface: Static IP Address” on page 143](#)
- [“External Interface: Static IP Address Configuration” on page 144](#)
- [“External Interface: DHCP Configuration” on page 145](#)
- [“External Interface: PPTP Client Configuration” on page 145](#)
- [“External Interface: L2TP Client Configuration” on page 146](#)
- [“External Interface: PPPoE Client Configuration” on page 147](#)

After you have configured the basic options for the internal IP interface, you can manage the security zones associated with the interface, or configure routing in the **Advanced Options** section. For details, see the following topics:

- [“Manage Security Zones for IP Interfaces” on page 149](#)
- [“Configuring Routing for IP Interfaces” on page 150](#)

Internal Interface: Static IP Address

The **Internal (LAN) Interfaces** on the X family device use static IP addressing.

When configuring Static IP addressing on the internal interfaces, you also have the option to allow the device to perform **Network Address Translation (NAT)**, which allows all the computers on your network to share one IP address.

Configure a Static IP Address on an Internal Interface

- STEP 1** From the LSM menu, select **Network > Configuration > IP Interfaces**.
- STEP 2** On the IP Interfaces page, click the **Create IP Interface** button or select the **Edit** icon for the interface that you want to edit.
- STEP 3** On the Edit/Create IP Interface page, select **Internal** as the Interface Type.
- STEP 4** Specify the **Internal Interface Configuration** information in the appropriate fields:
- **IP Address** — the address on the IP subnet that you have allocated for this interface
 - **Subnet Address** — the subnet mask associated with the IP subnet
- STEP 5** To allow all the computers on your network to share one IP address, check **Enable NAT**. Then, for the **Public NAT address**, either:
- Select **Use External Interface IP address**.
- OR**
- Select **Manually Enter** and enter a public IP address allocated by your ISP that is on the same subnet as the external interface.
- STEP 6** Click **Save**.
- Click **Cancel** to return to the NETWORK - Interfaces page without saving the changes.

After you have configured the basic options for the internal IP interface, you can manage the security zones associated with the interface, or configure routing in the **Advanced Options** section. For details, see the following topics:

- [“Manage Security Zones for IP Interfaces” on page 149](#)
- [“Configuring Routing for IP Interfaces” on page 150](#)

External Interface: Static IP Address Configuration

When configuring an external IP interface, you select **Static IP Address** if are using a public static IP address, or if your ISP has allocated you a public static IP address.



Note After configuring the External Interface as a static IP address, you need to configure the default gateway for the device from the Default Gateway page (**Network > Configuration > Default Gateway**). For details, see [“Default Gateway” on page 156](#).

Configure a Static IP Address on the External IP interface

STEP 1 Go to **Network > Configuration > IP Interfaces**.

STEP 2 On the IP Interfaces page, click the **Create IP Interface** button or select the **Edit** icon for the interface that you want to edit.

STEP 3 On the Create/Edit IP Interface page, select the **External** interface.



Note You can only configure one external interface on the device.

STEP 4 In the **External Interface Configuration** table, in the **External Interface Type** drop-down list field, select **Static**.

STEP 5 Type the following information in the appropriate fields:

- **IP Address** — the public static IP address that you are using or that has been allocated to you by your ISP for this connection.



Note If you have been allocated a range of IP addresses, enter one of the addresses in the range.

- **Subnet Mask** — the subnet mask allocated by your ISP for this connection.

STEP 6 Click **Save**.

Click **Cancel** to return to the IP Interfaces page without saving the changes.

After you have configured the basic options for the internal IP interface, you can manage the security zones associated with the interface, or configure routing in the **Advanced Options** section. For details, see the following topics:

- [“Manage Security Zones for IP Interfaces” on page 149](#)
- [“Configuring Routing for IP Interfaces” on page 150](#)

External Interface: DHCP Configuration

If your ISP has told you to use DHCP, or you are connecting to a device that provides the IP configuration for the device using DHCP, select **DHCP**. With DHCP, you can confirm the configuration settings by requesting a DHCP lease. If the interface is down, DHCP attempts to auto-connect until the connection establishes.

Configure DHCP on the External IP interface

- STEP 1** From the LSM menu, select **Network > Configuration > IP Interfaces**.
- STEP 2** On the IP Interfaces page, click **Create IP Interface** button or select the **Edit** icon for the interface that you want to edit.
- STEP 3** On the Create/Edit IP Interface page, select the **External** interface.



Note You can only configure one External Interface on the device.

- STEP 4** In the **External Interface Configuration** table, in the **External Interface Type** drop-down list field, select **DHCP**.
- STEP 5** Click **Save**.

Click **Cancel** to return to the IP Interfaces page without saving the changes.

After configuring the basic options for the internal IP interface, you can manage the security zones associated with the interface, or configure routing in the **Advanced Options** section. For details, see the following topics:

- [“Manage Security Zones for IP Interfaces” on page 149](#)
- [“Configuring Routing for IP Interfaces” on page 150](#)

External Interface: PPTP Client Configuration

Select **PPTP client** if your ISP is using PPTP to provide the IP configuration for the device, or you wish to use a PPTP tunnel for all WAN traffic (to connect back to the main office site, for example). After configuring the PPTP client, you can confirm the settings by pressing the **Connect** button.



Note Use of a PPTP client requires the device to have a valid IP configuration for the external Virtual Interface on the local network. This IP configuration can be provided by DHCP or specified via the "Local IP" parameters as shown in Step 6.

Configure PPTP client on the External IP interface

STEP 1 From the LSM menu, select **Network > Configuration > IP Interfaces**.

STEP 2 On the IP Interfaces page, click the **Create IP Interface** button or select the **Edit** icon for the interface that you want to edit.

STEP 3 On the Create/Edit IP Interface page, select **External** as the Interface Type.



Note You can only configure one External IP interface on the device.

STEP 4 In the **External Interface Configuration** table, in the **External Interface Type** drop-down list field, select **PPTP client**.

STEP 5 Enter the following information in the appropriate fields:

- **PPTP Server** — the IP address of the PPTP server provided by your ISP.
- **PPTP Username** — the user name allocated by your ISP for this connection.
- **PPTP Password** — the password allocated by your ISP for this connection.
- **Idle-Disconnect** — select the amount of time that a connection can be inactive before the user is logged out. Refer to your ISP for disconnect guidelines.

STEP 6 To set the Local IP Address on the external Virtual Interface allowing the device access to the IP network, either:

- Select **Local IP** — Use **DHCP** to use the Local IP Address allocated by the DHCP server.
- Select **Local IP — IP Address** and enter the following information to configure the connection manually:
 - IP Address** — the local WAN IP address of the device.
 - Subnet Mask** — the subnet mask of the WAN IP subnet.
 - Local Gateway** — the local gateway IP address for the WAN IP subnet.

STEP 7 Click **Save**.

Click **Cancel** to return to the IP Interfaces page without saving the changes.

After you have configured the basic options for the IP interface, you can manage the security zones associated with the interface, or configure routing in the **Advanced Options** section. For details, see the following topics:

- [“Manage Security Zones for IP Interfaces” on page 149](#)
- [“Configuring Routing for IP Interfaces” on page 150](#)

External Interface: L2TP Client Configuration

Select **L2TP client** if your ISP is using L2TP to provide the IP configuration for the device, or you wish to use an L2TP tunnel for all WAN traffic (to connect back to an HQ site, for example). After configuring the L2TP client, you can confirm the settings by pressing the **Connect** button.

Configure L2TP client on the External IP interface

STEP 1 From the LSM menu, select **Network > Configuration > IP Interfaces**.

STEP 2 On the IP Interfaces page, click the **Create IP Interface** button or select the **Edit** icon for the interface that you want to edit.

STEP 3 On the Create/Edit IP Interface page, select **External** as the Interface Type.



Note You can only configure one External Interface on the device.

STEP 4 In the **External Interface Configuration** table, in the **External Interface Type** drop-down list field, select **L2TP**.

STEP 5 Enter the following information in the appropriate fields:

- **L2TP Server** — the IP address of the L2TP server provided by your ISP.
- **L2TP Username** — the user name allocated by your ISP for this connection.
- **L2TP Password** — the password allocated by your ISP for this connection.
- **Disconnect** — select the amount of time that a connection can be inactive before the user is logged out. Refer to your ISP for disconnect guidelines.

STEP 6 To set the Local IP Address on the external Virtual Interface allowing the device access to the IP network, either:

- Select **Use DHCP** to use the Local IP Address allocated by the DHCP server.
- Select **IP Address** and enter the following information to configure the connection manually:
 - IP Address** — the local WAN IP address of the device.
 - Subnet Mask** — the subnet mask of the WAN IP subnet.
 - Local Gateway** — the local gateway IP address for the WAN IP subnet.

STEP 7 Click **Save**.

Click **Cancel** to return to the NETWORK - Interfaces page without saving the changes.

After you have configured the basic options for the IP interface, you can manage the security zones associated with the interface, or configure routing in the Advanced Options section. For details, see the following topics:

- [“Manage Security Zones for IP Interfaces” on page 149](#)
- [“Configuring Routing for IP Interfaces” on page 150](#)

External Interface: PPPoE Client Configuration

If your ISP is using PPPoE to provide the IP configuration for the device, select **PPPoE client**. After configuring the PPPoE client, you can confirm the settings by pressing the **Connect** button.

Configure PPPoE client on the External IP interface

STEP 1 From the LSM menu, select **Network > Configuration > IP Interfaces**.

STEP 2 On the IP Interfaces page, click the **Create IP Interface** button or select the **Edit** icon for the interface that you want to edit.

STEP 3 On the Create/Edit IP Interfaces page, select the **External** interface.



Note You can only configure one External Interface on the device.

STEP 4 In the **External Interface Configuration** table, in the **External Interface Type** drop-down list field, select **PPPoE**.

STEP 5 Enter the following information in the appropriate fields:

- **Username** — the user name allocated by your ISP for this connection.
- **Password** — the password allocated by your ISP for this connection.
- **Disconnect** — select the amount of time that a connection can be inactive before the user is logged out. Refer to your ISP for disconnect guidelines.

STEP 6 Click **Save**.

Click **Cancel** to return to the Network - Interfaces page without saving the changes.

After you have configured the basic options for the IP interface, you can manage the security zones associated with the interface, or configure routing in the **Advanced Options** section. For details, see the following topics:

- [“Manage Security Zones for IP Interfaces” on page 149](#)
- [“Configuring Routing for IP Interfaces” on page 150](#)

Configuring a GRE Tunnel

An IP Security (IPSec) tunnel can only carry unicast IP traffic. **Generic Route Encapsulation (GRE)** can be used to allow transfer of dynamic routing (RIP) and multicast traffic between two GRE end points (a GRE tunnel). This GRE tunnel can then be secured by further encapsulation within an IPSec tunnel. Note that GRE tunnels cannot encapsulate non-IP traffic.



Note For secure GRE connections, you must configure an IPSec Security Association (IPSec SA) before you configure GRE tunnels. You can configure an IPSec SA from the IPSec Status page (**VPN > IPSec Status**).

The GRE tunnel requires a security zone.

Configure a GRE Tunnel to a Remote Device

- STEP 1** From the LSM menu, select **Network > Configuration > IP Interfaces**.
- STEP 2** On the IP Interfaces page, click **Create IP Interface** or select the **Edit** icon for the interface that you want to edit.
- STEP 3** On the Create/Edit IP Interfaces page, click **GRE Tunnel secured by IPSec SA** as the Interface Type. Then, select the Security Association from the drop-down list.
- STEP 4** Complete the **GRE Interface Config** as follows:
- STEP A** In the **Remote Tunnel Endpoint**, type the IP address for the remote device on the public network.
- STEP B** In the **IP Address** field, enter the IP address of the tunnel on the local network on the external virtual interface. Choose an unused IP address that is routable through your network.
- STEP C** In the **Peer IP Address** field, type the IP address for the peer. This is the IP address entered in the IP Address field on the remote device.
- STEP 5** In the Security Zones table, configure the security zones assigned to the tunnel. For details, see [“Manage Security Zones for IP Interfaces” on page 149](#).
- STEP 6** Click **Save**.

Click **Cancel** to return to the Network - Interfaces page without saving the changes.

After you have configured the basic options for the GRE tunnel, you can manage the security zones associated with the interface, or configure routing in the **Advanced Options** section. For details, see the following topics:

- [“Manage Security Zones for IP Interfaces” on page 149](#)
- [“Configuring Routing for IP Interfaces” on page 150](#)

Manage Security Zones for IP Interfaces

Security Zones can be configured to control traffic across the network. Each security zone is associated with an IP interface.

The IP Interfaces page lists the zones that are assigned to each interface. Layer 2 Firewalling and IPS Filtering can be applied between any two security zones even if they are on the same IP interface.


You can manage (add or remove) the Security Zone configuration for an IP interface from the Edit/Create IP Interface page.

Manage (add or remove) Security Zones for IP Interfaces

- STEP 1** From the LSM menu, select **Network > Configuration > IP Interfaces**.
- STEP 2** On the IP Interfaces page, click the **Create IP Interface** button or select the **Edit** icon for the interface that you want to edit.
- STEP 3** On the Create/Edit IP Interfaces page, scroll down to the **Security Zone** table.

STEP 4 From the **Security Zone** drop-down list, select the zone you want to add to the IP interface. Then, click **add to table below**.

Add as many zones as needed.

STEP 5 To delete a zone, in the **Function(s)** column for the zone, click  .

STEP 6 Click **Save**.

Click **Cancel** to return to the IP Interfaces page without saving the changes.

Configuring Routing for IP Interfaces

You can configure IP interfaces to perform dynamic unicast or multicast routing if required. You can modify routing information from the Create/Edit IP Interfaces page (**Network > Configuration > IP Interfaces**). For details, see the following topics:

- [“Bridge Mode for IP Interfaces” on page 150](#)
- [“RIP for IP Interfaces” on page 150](#)
- [“Multicast Routing for IP Interfaces” on page 152](#)

Bridge Mode for IP Interfaces

In bridge mode, the X family device implements a software bridge to transparently connect security zones assigned to the same virtual interface. Using bridge mode, you do not have to configure IP routes to bridge traffic.



Note The High Availability feature is not available if bridge mode is enabled.

Enable Bridge Mode on an IP Interface

STEP 1 From the LSM menu, select **Network > Configuration > IP Interfaces**.

STEP 2 On the IP Interfaces page, click the **Create IP Interface** button or select the **Edit** icon for the interface that you want to edit.

STEP 3 On the Create/Edit IP Interfaces page, scroll down to **IP Interface Details (Advanced)** table. If the table is not displayed, click **Show Advanced Options**.

STEP 4 Click the **Enable bridge mode** check box.

STEP 5 Click **Save**.

Click **Cancel** to return to the Network - Interfaces page without saving the changes.

RIP for IP Interfaces

RIP (Routing Information Protocol, RFC 2453) is used for exchanging unicast routing information between routers and hosts.

The device listens for RIP advertisements from other routers and combines this with its static route and configured interface information, then calculates the shortest route to any destination.

Using RIP, the device determines the route for network packets based on the fewest number of hops between the source and the destination. RIP regularly broadcasts routing information to other devices on the network

RIPv1 Configuration Settings

RIPv1 is a simple distance vector protocol where the longest path cannot exceed 15 hops and static metrics are used to compare routes. RIPv1 should only be used to communicate routing information with legacy devices that cannot support RIPv2. Because the protocol does not send subnet mask information, it is considered technically obsolete and can cause routing problems in classless networks. RIPv1 should only be used when all of the consequences of its use are well understood by the network administrator.

RIPv2 Configuration Settings

RIP version 2 is the current version of the RIP protocol. It adds support subnetted CIDR networks and authentication of routing updates. The preferred method for sending RIPv2 advertisements is multicast. This also reduces the interrupt load on other network devices that are not interested in routing updates. Broadcast should only be used for compatibility with legacy RIPv1 devices. RIPv2 MD5 authentication is highly recommended to prevent the device from accepting bogus routing information.



Note Before using RIP on an IP Interface, you must enable it globally from the RIP Setup page (**Network > Routing > RIP**).

Enable and Configure RIP on an IP Interface

- STEP 1** From the LSM menu, select **Network > Configuration > IP Interfaces**.
- STEP 2** On the IP Interfaces page, click the **Create IP Interface** button or select the **Edit** icon for the interface that you want to edit.
- STEP 3** On the Create/Edit IP Interfaces page, scroll down to **IP Interface Details (Advanced)** table. If the table is not displayed, click **Show Advanced Options**.
- STEP 4** In the **RIP table**, click the **Enable RIP** check box.
- STEP 5** To prevent this interface being advertised by RIP throughout the network, check **Disable RIP Advertisement of this interface on other interfaces**.
We recommend enabling this option on the External IP interface.
- STEP 6** Select one of the following from the **Send** mode drop-down list:
 - **Do not send updates** — passive mode
 - **RIP v1** — send route advertisements as RIPv1
 - **RIP v2 Multicast** — send route advertisements using IP multicast address 224.0.0.9
 - **RIP v2 Broadcast** — send route advertisements using IP broadcast address

STEP 7 Select one of the following from the **Receive** mode drop-down list:

- **Do not receive updates** — Ignore all route advertisements received on this interface.
- **RIP v1 only** — Accept only v1 advertisements received on this interface.
- **RIP v2 only** — Accept only v2 advertisements received on this interface.
- **RIP v1 or v2** — Accept any RIP advertisements received on this interface.

STEP 8 For **RIP v2 Authentication**, select one of the following authentication methods:

- **None** — Use no authentication of RIP communication on the interface.
- **Simple** — Use clear text password authentication. Enter a password of between 1 and 32 characters (over 8 characters recommended).
- **MD5** — Use Message Digest version 5 (MD5) authentication. Enter a password of between 1 and 32 characters (over 8 characters recommended). MD5 is the recommended authentication mechanism.

STEP 9 Check **Enable Split Horizon** to prevent routers from advertising networks in the direction from which those networks were learned.

Split Horizon reduces convergence time by not allowing routers to advertise networks in the direction from which those networks were learned. The announcements only include networks in the opposite direction. This also reduces loops.

STEP 10 If **Split Horizon** is enabled, select **Poison Reverse** to further ensure that routes learned from a neighbor are not advertised back.

Routes learned from a neighbor are advertised back to it with metric 16 (unreachable). Enabling Poison Reverse has a similar effect as split horizon, and is also called split horizon with poison reverse. In a single-path network this has no advantage over split horizon. However, in multi-path networks this greatly reduces loops.

STEP 11 Click **Save**.

Click **Cancel** to return to the Network - Interfaces page without saving the changes.

Multicast Routing for IP Interfaces

The device can be configured to function as a multicast router on the network.

The device supports two multicast protocols. You can configure an IP interface with either or both protocols.

- **IGMP — Internet Group Management Protocol**, used by hosts to define multicast group membership. Multicast groups are identified by special IP addresses.
IGMP must be enabled on all IP interfaces that are directly connected to clients using multicast traffic.
- **PIM-DM — Protocol Independent Multicast-Dense Mode** routing protocol, used for multicast routing between remote sites. PIM-DM is also used to support site-to-site NBX conference calls.
PIM-DM must be enabled on all IP interfaces that multicast data will travel through to/from the multicast clients. This includes the GRE and IP interfaces.



Note Firewall rules must be established to allow PIM-DM and IGMP to be passed through the firewall between each set of security zone pairs that the multicast traffic must traverse. This includes between virtual zones such as a VPN zone, and this-device.

Enable Multicasting on an IP Interface

- STEP 1** From the LSM menu, select **Network > Configuration > IP Interfaces**.
- STEP 2** On the IP Interfaces page, click the **Create IP Interface** button or select the **Edit** icon for the interface that you want to edit.
- STEP 3** On the IP Interfaces (Create/Edit) page, click the **Enable IGMP** and/or **Enable PIM-DM** check box to enable multicast routing.
- STEP 4** Click **Save**.
Click **Cancel** to return to the IP Interfaces page without saving the changes.
- STEP 5** Enable Firewall Rules to allow PIM-DM and/or IGMP to/from *this-device* for the relevant zones.

After configuring the multi-cast routing options, verify the IGMP and/or PIM-DM options have been enabled globally. For details, see the following topics:

- [“IGMP Setup” on page 163](#)
- [“PIM-DM Setup” on page 165](#)

IP Address Groups

IP Address Groups allow you to associate a selection of IP addresses with a name that can be used in place of the specific IP addresses. IP Address Groups save time when configuring features on the device since you can apply the same parameters to all IP addresses in the group rather than configuring each address separately.

IP Address Groups can be used when configuring the following features:

- Firewall rules
- DHCP server address pool
- IPSec local and destination subnets
- PPTP pool
- L2TP pool
- Security zones

You can manage IP Address Groups from the IP Address Groups page (**Network > Configuration > IP Address Groups**).

From this page you can complete the following tasks:

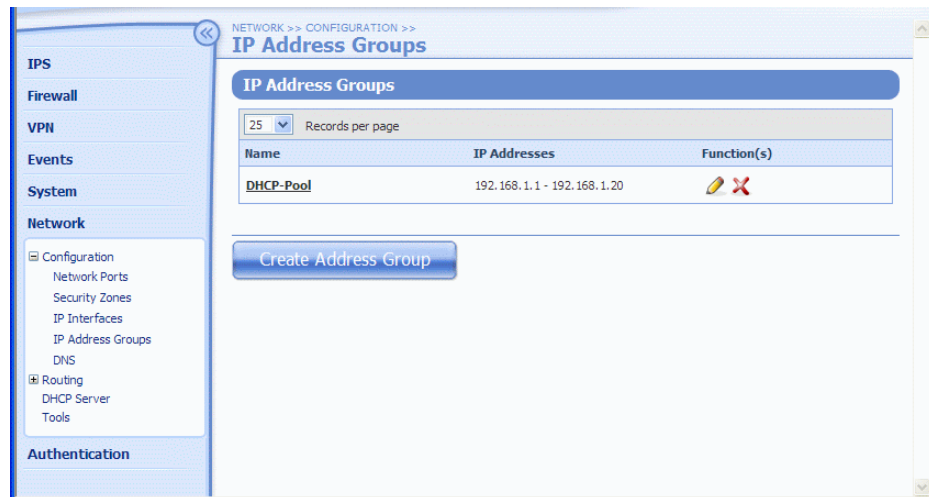
- Create an IP Address Group
- Edit an existing group to add or remove addresses
- Delete an IP Address Group

For additional information, see the following:

- [Table 6–3, “IP Address Group Details,” on page 155](#)
- [“Create or Edit IP Address Groups” on page 155](#)



The following figure shows the IP Address Groups page:

Figure 6–8: Network: Configuration: IP Addresses Page



The IP Address Groups page provides the following information about existing groups:

Table 6-3: IP Address Group Details

Column	Description
Name	The name of the IP Address Group
IP Addresses	The IP addresses belonging to the group. These can include IP hosts, IP ranges and IP subnets
Function(s) The functions available to manage each IP Address Group listed in the table: <ul style="list-style-type: none">  • Delete an IP Address Group  • Edit the IP Address Group to add or remove IP addresses. 	

Create or Edit IP Address Groups

- STEP 1** From the LSM, select **Network > Configuration > IP Address Groups**.
- STEP 2** On the IP Address Groups page, click the Create/Edit page to add an IP Address Group, or click the Edit button for the group you want to edit.
- STEP 3** On the Create/Edit IP Address Group page, type a **Group Name**.
- STEP 4** Select the type of IP Address you want to add to the group, either:
- **IP Host** — a host IP address.
 - **IP Subnet** — a subnet IP address/mask.
 - **IP Range** — a range of IP addresses.
- STEP 5** Click **Add to table below** to add the address to the group and update the table.
- To remove an address, click the Delete icon in the **Function(s)** column of the address table.
- STEP 6** Click **Save**.

DNS

You can configure the global DNS servers and search domains for the device from the DNS page (**Network > Configuration > DNS**). You can configure up to three DNS servers and search domains, or use the DNS configuration obtained from the WAN connection.

Manually Configure the Global DNS Servers

- STEP 1** From the LSM menu, select **Network > DNS**.
- STEP 2** On the DNS page, select **Manually configure DNS servers and search domains**.
- STEP 3** Type the **DNS Server** and **Search Domain** for up to three DNS servers.
- STEP 4** Click **Apply**.

Obtain DNS Configuration from WAN Connection

STEP 1 From the LSM menu, select **Network > DNS**.

STEP 2 On the DNS page, select **Use DNS configuration from WAN connection**.

When this option is selected, the DNS server configuration returned from the ISP will be used. Alternatively, the DNS servers can be explicitly set using the manual configuration option.

STEP 3 Click **Apply**.



Note If you have enabled and configured the DHCP server option for the device, you can override the DNS settings returned to DHCP clients if necessary. For details, see [“Configure DHCP Server” on page 169](#). If you do not override these settings, DHCP clients will receive the DNS server settings used by the device itself.

Default Gateway

If you have configured the External Interface to use a static IP address, then you must manually configure the default gateway. The device uses the default IP gateway to route packets when it has no other route to a given IP address.



Note If you are using L2TP, PPTP, PPPoE, or DHCP, then the default route will be automatically configured by your ISP and you cannot configure it yourself.

Configure the Default Route

STEP 1 Go to **Network > Configuration > Default Gateway**.

STEP 2 On the Default Gateway page in the **Manually configure Default Gateway** field, type the **IP Address** for the default gateway.

Enter the IP address of the next router on the WAN side of the device into the **Default Gateway** field. Your ISP will provide you with this information.

Routing

Overview

The device provides static and dynamic routing which can be managed and configured from the Routing menu pages. The menu provides the following options:

- **Routing Table** — View all current routes on the device. Use the Routing Table to view the routes by IP Address and Subnet Mask.
- **Static Routes** — Review, manage and create static routes for the device. A **Static Route** defines the gateway to use for a particular network.
- **RIP** — Enable RIP (unicast routing) globally, view and edit IP interfaces configured with RIP.
- **IGMP** — Enable IGMP (multicast routing) globally, view and edit IP interfaces configured with IGMP.
- **PIM-DM** — Enable PIM-DM (multicast routing) globally, view and edit IP interfaces configured with IGMP.



Note If you have configured RIP, IGM, PIM-DM routing on an IP Interface, these options must be enabled globally in order for the routing to be implemented.

For additional information, see the following topics:

- [“Routing Table” on page 157](#)
- [“Configure the Default Route” on page 156](#)
- [“Static Routes” on page 159](#)
- [“RIP for IP Interfaces” on page 150](#)

Routing Table

Use the Routing Table page (**Network > Routing > Routing Table**) to view all current routes on the device by IP Address and Subnet Mask. The table displays up to 250 routes.

From the routing table page, you can:

- Click on a column heading to sort the table by the specified parameter: **Destination IP, Subnet Mask, Next Hop, Metric, Age, and Status**.
- Select a **Records per page** setting to change the number of routing entries displayed in the table.
- Click **Refresh** to update the table with the most current network information.



Note Routes across a VPN are always the most specific. There is no way to configure a static route, or a route learned via RIP to override a VPN route.

The following figure shows the Routing Table page:

Figure 6–9: Network Configuration: Routing Table Page

Destination	Subnet Mask	Next Hop	Metric	Age	Status
Default	0.0.0.0	10.134.2.2	8	0	static
10.134.2.0	255.255.255.0	10.134.2.254	1	0	direct
10.134.2.254	255.255.255.255	127.0.0.1	1	0	local
10.100.0.0	255.255.0.0	10.100.34.100	1	0	direct
10.100.34.100	255.255.255.255	127.0.0.1	1	0	local
10.134.1.0	255.255.255.0	10.134.1.254	1	0	direct
10.134.1.254	255.255.255.255	127.0.0.1	1	0	local
152.67.136.0	255.255.255.0	10.100.0.254	1	0	static
152.67.137.0	255.255.255.0	10.100.0.254	1	0	static
152.67.138.0	255.255.255.0	10.100.0.254	1	0	static
152.67.139.0	255.255.255.0	10.100.0.254	1	0	static
152.67.140.0	255.255.255.0	10.100.0.254	1	0	static
216.136.56.0	255.255.255.0	10.100.0.254	1	0	static
216.136.107.0	255.255.255.0	10.100.0.254	1	0	static
127.0.0.0	255.0.0.0	127.0.0.1	1	0	local

The **Network - Routing Table** provides the following information:

Column	Description
Destination	The IP address of the destination network
Subnet Mask	The subnet mask of the destination network
Next Hop	The IP address of the router that will be used to access a host or subnet.
Metric	The number that is used to determine the order in which the static route will be accessed
Age	The number of seconds since the route entry appeared in the Routing Table. For permanent routes (local, direct, and static) a hyphen (-) is displayed
Status	One of the following: <ul style="list-style-type: none"> • Static if the route is to the default destination • Local if the route is a device IP address • Direct if the route is directly attached to an IP interface on the subnet

Static Routes

A **Static Route** defines the gateway to use for a particular network. The device supports the use of static routes to forward traffic:

- Between the device and any external interface, for example, you may need to define a static route so that the device can communicate with the email server used to send event notifications.
- Between the device and any GRE interface.



Note Static routes configured on the device are not used to route traffic to subnets at the other end of an IPSec VPN tunnel. The destination network's configuration in the Security Association associated with a VPN tunnel is used for this. For more information, see [“Edit the Default SA for Client-to-Site VPN Connections using L2TP over IPSec” on page 194.](#)

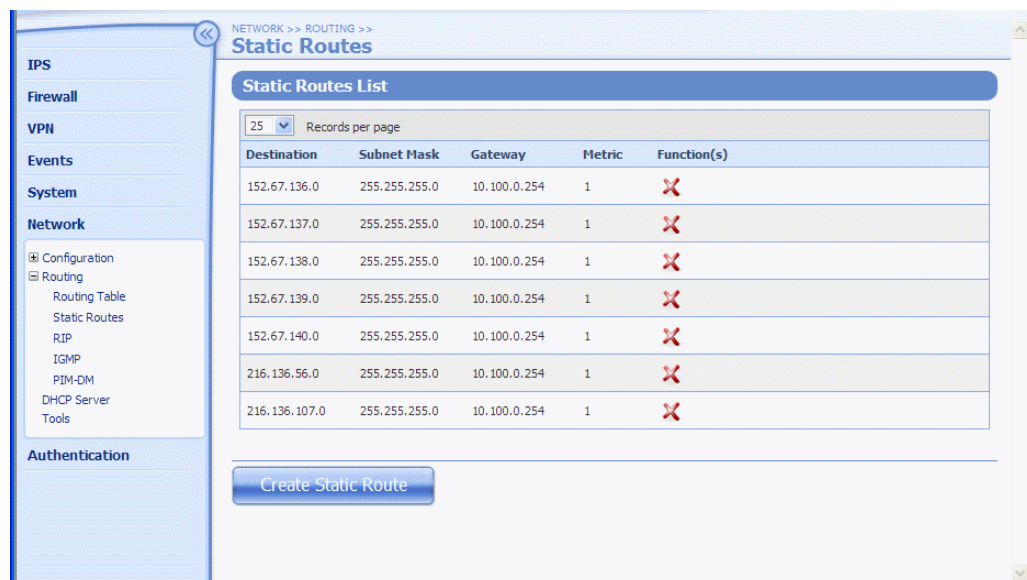
Routes across a VPN are always the most specific. There is no way to configure a static route, or a route learned via RIP to override a VPN route.

You can view and manage static route from the Static Routes page (**Network > Configuration > Static Routes**). From this page you can:

- View the list of existing routes
- Select a **Records per page** setting to change the number of static route entries displayed in the table
- Delete a static route
- Create a static route

The following figure shows the Static Routes page:

Figure 6–10: Network Configuration: Static Routes Page



The Static Routes page provides the following information:

Column	Description
Destination	The IP address of the destination network for the static route
Subnet Mask	The subnet mask of the destination network
Gateway	The IP address of the device to which the device forwards traffic destined for the destination network
Metric	<p>A number (between 1 and 15) that is used to determine the order in which the static route will be accessed.</p> <p>Note By default, the device will re-distribute any static routes configured on the device into RIP. If you do not want to re-distribute some static routes, configure those with a metric of 15. The other peer routers will receive these routes, increment the metric by one (to 16). RIP routes with a metric of 16 are considered unreachable and will be discarded by the peer router.</p>

Create a Static Route

STEP 1 From the LSM menu, select **Network > Configuration > Static Routes**.

STEP 2 On the Static Routes page, click **Create Static Route**.

STEP 3 On the Create Static Route page, type the **IP Address** of the destination network.



Note Setting this address to 0.0.0.0 is not allowed.

STEP 4 Type the **Subnet Mask** of the destination network.

STEP 5 Type the **Gateway IP address**.

For GRE tunnels, enter the IP address for the tunnels.

STEP 6 Type the **Metric** for this route.

Enter a number between 1 and 15 that represents the priority of this static route which determines the order in which the route will be accessed. To prevent the static route from being re-distributed when RIP is enabled on the device, enter 15.

STEP 7 Click **Create** to add the static route and update the current Static Routes table.

RIP Setup

Routing Information Protocol (RIP) is used for exchanging unicast routing information between routers and hosts. Using RIP, the device determines route for network packets based on the fewest

number of hops between the source and the destination. RIP regularly broadcasts routing information to other devices on the network.



CAUTION When RIP is enabled, the device automatically re-distributes any static routes configured on the device into RIP. If you do not want to re-distribute some static routes, configure those with a metric of 15. The other peer routers will receive these routes, increment the metric by one (to 16). RIP routes with a metric of 16 are considered unreachable and will be discarded by the peer router.

You can manage and configure RIP routing from the RIP Setup page (**Network > Configuration > RIP**). From this page you can:

- View the current RIP configuration for the device and the current state of RIP for each IP interface.
- Enable RIP globally on the device and set the routing timer.
- Edit the RIP configuration for an IP interface.

This following figure shows the RIP Setup page:

Figure 6–11: Network Configuration: RIP Setup Page

On the RIP Setup page, the **Interfaces Setup** table lists the existing interfaces on the device, and provides the following information about the RIP configuration on each interface:

Column	Description
State	Whether RIP is enabled or disabled on the interface. Generally, RIP should not be enabled on the external interface.
Send Mode	The mode used for broadcasting the routing information, either v1 , v2 Broadcast , v2 Multicast or Disabled
Receive Mode	The mode used for receiving the routing information, either v1 only , v2 only , v1 or v2 or Disabled

Column	Description
Split Horizon	Whether Split Horizon is enabled or disabled on the interface. Split Horizon reduces convergence time by not allowing routers to advertise networks in the direction from which those networks were learned. The announcements only include networks in the opposite direction. This also reduces loops.
Poison Reverse	Whether Poison Reverse is enabled or disabled on the interface. If Poison Reverse is enabled routes learned from a neighbor are advertised back to it with metric 16 (unreachable). This has a similar effect as split horizon, and is also called split horizon with poison reverse. In a single-path network this has no advantage over split horizon. However, in multi-path networks this greatly reduces loops.
Authentication	The type of authentication used on the interface, either none , MD5 or Simple .
Function(s)	The functions available to manage IP interface. Edit is the only option available.

For additional information, see the following topics:

- [“Enable RIP Globally” on page 162](#)
- [“Edit the Configuration of RIP on a IP Interface” on page 162](#)
- [“Managing IP Interfaces” on page 141](#)

Enable RIP Globally

STEP 1 From the LSM, select **Network > Routing > RIP**. The NETWORK - RIP Setup page displays.

STEP 2 On the RIP Setup page, check **Enable RIP**.

This globally enable RIP such that it can be used on any interface.



Note You must enable RIP globally in order to run it on any interface. Generally, you should not enable RIP on external IP interfaces.

STEP 3 In the **Routing Update Timer** field, enter a value between 1 and 600 seconds (default 30 seconds) for the interval between updates of RIP routes to neighbors.

STEP 4 Click **Apply** to save the change.

Edit the Configuration of RIP on a IP Interface

STEP 1 From the LSM menu, select **Network > Routing > RIP**.

STEP 2 On the RIP Setup page, click the **Edit** icon for the interface you want to edit.

STEP 3 On the Edit IP Interfaces page in the **Advanced Options** section, modify the RIP configuration as required.

STEP 4 Enable Firewall Rules to allow RIP to/from *this-device* for the relevant zones.

For more information on configuring interfaces, see [“Enable Bridge Mode on an IP Interface” on page 150](#).

Multicast (IGMP and PIM-DM)

The device can act as an IP multicast router, supporting IGMP and PIM-DM multicast protocols.

- **IGMP — Internet Group Management Protocol**, used by hosts to define multicast group membership. Multicast groups are identified by special IP addresses.
IGMP must be enabled on all IP interfaces that are directly connected to clients using multicast traffic.
- **PIM-DM — Protocol Independent Multicast-Dense Mode** routing protocol, used for multicast routing between remote sites. PIM-DM is also used to support site-to-site NBX conference calls.
PIM-DM must be enabled on all IP interfaces that multicast data will travel through to/from the multicast clients. This includes the GRE and IP interfaces.



Note Firewall rules must be established to allow PIM-DM and IGMP to be passed through the firewall between each set of security zone pairs that the multicast traffic must traverse. This includes between virtual zones such as a VPN zone, and this-device.

IGMP Setup

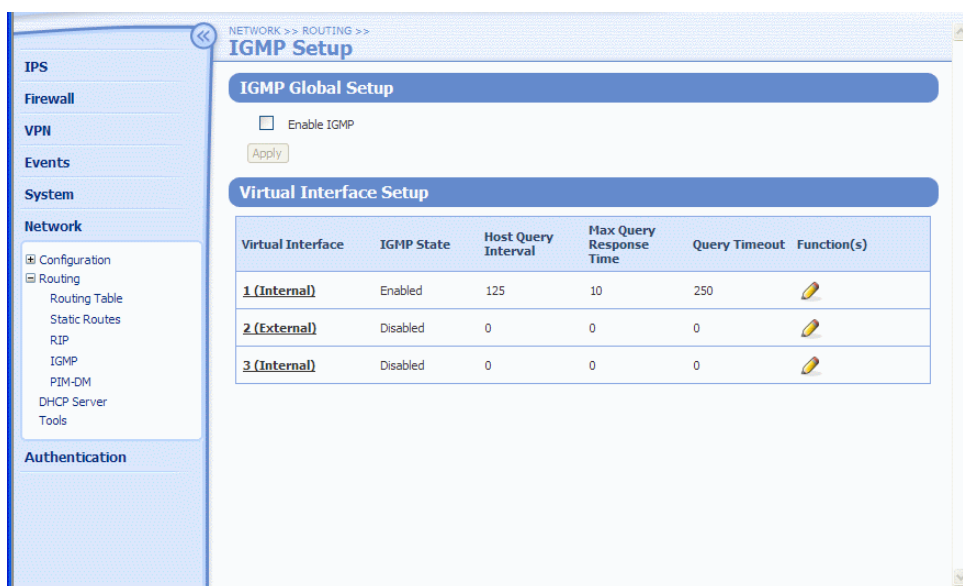
Internet Group Management Protocol (IGMP) is used by hosts to join or leave multicast groups.

You can manage and configure IGMP routing from the IGMP Setup page (**Network > Configuration > IGMP**). From this page you can:

- View the current IGMP configuration for the device and the current state of IGMP for each IP interface.
- Configure the global IGMP setup parameters for the device.
- Edit the IGMP configuration for an IP interface.

This following figure shows the IGMP Setup page:

Figure 6–12: Network Configuration: IGMP Setup Page



On the IGMP Setup page, the **IP Interfaces Setup** table lists the existing interfaces on the device, and provides the following information about the IGMP configuration on each interface:

Column	Description
IGMP State	Whether IGMP is enabled or disabled on this IP interface.
Host Query Interval	Interval in seconds between queries from the IGMP querier router to multicast groups. Default interval is 125 seconds.
Max Query Response Time	Maximum time that the querier waits for a response from the host.
Query Timeout	Length of time that the interface waits for a query from the host before it becomes the querier. Default is double the Host Query Interval.

For additional information, see the following topics:

- [“Enable IGMP Globally” on page 165](#)
- [“Edit IGMP Configuration on an IP Interface” on page 165](#)
- [“Managing IP Interfaces” on page 141](#)

Enable IGMP Globally

STEP 1 From the LSM, select **Network > Routing > IGMP**.

STEP 2 On the IGMP Setup page, check **Enable IGMP**.



Note You must enable IGMP globally in order to run it on an interface.

STEP 3 Click **Apply** to save the change.

Edit IGMP Configuration on an IP Interface

STEP 1 From the LSM, select **Network > Routing > IGMP**.

STEP 2 On the IGMP Setup page, in the **IP Interfaces Setup** table, click the **Edit** icon for the interface you want to edit. Then, configure IGMP for the interface.

STEP 3 Enable Firewall Rules to allow IGMP to/from *this-device* for the relevant zones.

For more information on configuring interfaces, see [“Enable Multicasting on an IP Interface” on page 153](#).

PIM-DM Setup

Protocol Independent Multicast-Dense Mode (PIM-DM) is used for multicast routing between remote sites.

You can manage and configure PIM-DM routing from the PIM-DM Setup page (**Network > Configuration > IGMP**). The IP Interfaces Setup table lists the existing IP interfaces on the device, and indicates whether PIM-DM is enabled or disabled on this IP interface. From this page you can:

- View the current PIM-DM configuration for the device and the current state of PIM-DM for each IP interface.
- Configure the global PIM-DM setup parameters for the device.
PIM-DM must be enabled on interfaces that are connected to another multicast router that separates the device from clients using multicast traffic.
- Edit the PIM-DM configuration for an IP interface.

This following figure shows the PIM-DM Setup page:

Figure 6–13: Network Configuration: PIM-DM Setup Page

NETWORK >> ROUTING >> PIM-DM Setup

PIM-DM Global Setup

☐ Enable PIM-DM

Query Interval: 30 seconds

Prune Timeout: 180 seconds

Apply

Virtual Interface Setup

Virtual Interface	PIM-DM State	Function(s)
1 (Internal)	Enabled	
2 (External)	Disabled	
3 (Internal)	Disabled	

Enable PIM-DM globally

STEP 1 Check **Enable PIM-DM**.



Note You must enable PIM-DM globally in order to run it on an interface.

STEP 2 Enter a value between 1 and 600 seconds (default 30 seconds) for the **Query Interval**.

STEP 3 Optionally, enter a value between 1 and 900 seconds (default 180 seconds) for the **Prune Timeout**.

Prune Timeout alleviates some PIM-DM flood problems. A prune delay is introduced, allowing the first multicast packet to flood to all sites. Subsequent multicast packets to that multicast group are then dropped until most prunes have returned from remote devices, when the multicast stream is released again.

STEP 4 Click **Apply** to save the change.

Edit PIM-DM Configuration on an IP Interface

STEP 1 From the LSM menu, select **Network > Configuration > PIM-DM**.

STEP 2 On the PIM-DM Setup page in the **IP Interfaces Setup** table, click the **Edit** icon for the interface you want to edit. Then, configure PIM-DM for the interface.

STEP 3 Enable Firewall Rules to allow PIM-DM to/from *this-device* for the relevant zones.

For more information on configuring interfaces, see [“Enable Multicasting on an IP Interface” on page 153](#).

Default Gateway

The default gateway is the route to which the device will forward any packet whose destination address it does not recognize. You configure this route when you configure the external interface.



Note If you are using PPPoE or DHCP, then the default route will be automatically configured by your ISP and you cannot configure it yourself.

Configure the Default Route

1. Go to **Network > Interfaces**. The NETWORK - Interfaces page opens.
2. Locate the external interface and click the **Edit** icon.
3. Enter the IP address of the next router on the WAN side of the device into the **Default Gateway** field. Your ISP will provide you with this information.

DHCP Server

Overview

A DHCP server allows computers on your network to obtain an IP address and subnet mask automatically. DHCP assigns a temporary IP address and subnet mask to any PC that requires IP configuration information. When a PC with a DHCP-assigned address disconnects from the network, the address is released and can be re-assigned.

You can configure the device to act as a DHCP server for devices on its LAN-side interfaces (internal IP interfaces) that require IP configuration. The following DHCP Server menu pages (**Network > DHCP Server**) are available to manage and configure DHCP settings:



Note The DHCP server is enabled by default and configured with the default IP Address Group DHCP-Pool which includes 20 IP addresses in the subnet defined for the internal IP interface. These DHCP addresses are 192.168.1.1 - 192.168.1.20. You can disable the DHCP server or modify the configuration based on your network requirements.

- **DHCP Server Summary Page** — view the current status of DHCP leases and a list of current DHCP clients.
- **Static Reservations** — create and manage static mappings on the device. A static mapping is used to assign a specific IP address to a device such as a printer or DNS server.
- **DHCP Relay** — enable and configure the DHCP Relay option on the device.
- **Configure DHCP** — enable the DHCP server option and configure the settings.

For additional information, see the following topics:

- [“DHCP Server Page” on page 168](#)
- [“DHCP Relay” on page 171](#)
- [“Static Reservations” on page 174](#)
- [“Configure DHCP Server” on page 169](#)

DHCP Server Page

DHCP Server leases the IP addresses to the DHCP clients. If a lease has not been released normally, you can release it manually. By default, the device DHCP server grants leases for one hour. You can edit the duration of the lease on the Configure DHCP page. If you are running short of addresses in the DHCP Pool and know that some computers are unlikely to connect to the network soon, you can release the IP address allowing it to be reallocated to another PC.


DHCP lease assignments are generally stable even if the client and devices are rebooted. The same client usually gets the same DHCP lease when it devices come back online unless that is prevented for some reason (e.g. all the leases are used up or the lease in question is otherwise in use).

Use the DHCP Server page to complete the following tasks:

- View current and available leases
- View a list of current clients with DHCP-allocated addresses
- Release a client IP address so that the IP address can be reallocated
- Access the functions to manage Static Reservations, DHCP Relay, and DHCP Configuration

The **DHCP Client Summary** table provides the following information about the status of current DHCP client leases:

Table 6–4: Network: DHCP Server Details

Column	Description
IP Address	The IP address assigned from the DHCP Address Pool
Host Name	The host name of the client
MAC Address	The MAC address of the client
Type	Either Dynamic for a lease from the DHCP Address Pool, Static if Static Mapping has been applied, or Dynamic (BOOTP) for a BOOTP client
Function(s) 	The available functions for DHCP Clients: <ul style="list-style-type: none"> • Release the client so that the DHCP address can be reallocated.

For additional information, see the following topics:

- [“Release a DHCP Lease” on page 169](#)
- [“Configure DHCP Server” on page 169](#)
- [“DHCP Relay” on page 171](#)
- [“Static Reservations” on page 174](#)

Release a DHCP Lease

STEP 1 From the LSM menu, select **Network > DHCP Server**.

STEP 2 On the DHCP Server page in the **DHCP Client Summary** table, click the **Release** icon to end the lease and update the table.

Configure DHCP Server

You can configure the device to be your DHCP server, thereby allowing computers on your network to obtain an IP address and subnet mask automatically.



Note Ensure that the firewall rules configured on the device allow DHCP clients to send DHCP requests to the correct security zone and to receive their IP address by DHCP. For details, see [“Firewall” on page 63](#).

Default DHCP Configuration

The DHCP server is enabled by default and configured with the default IP Address Group DHCP-Pool which includes 20 IP addresses in the subnet defined for the internal IP interface. These DHCP addresses are 192.168.1.1 - 192.168.1.20. The default lease duration is one hour. You can disable the DHCP server or modify the default configuration based on your network requirements.

You can view and manage the DHCP configuration on the DHCP Configuration page (**Network > DHCP Server > Configure DHCP**). From this page, you can complete the following tasks:

- Enable/disable DHCP
- Change the lease duration
- Configure the DHCP Address Pool from which the device allocates addresses
- Select DHCP server options for DNS, WINS, and NBX services

Enable and Configure the DHCP Server

STEP 1 From the LSM menu, select **Network > DHCP Server**. Then, click the **Configure DHCP** tab.

STEP 2 On the Configure DHCP Server page, check **Enable DHCP Server** to enable the DHCP server. Then, configure the following options as required:

- In the **Lease Duration** field, enter a value between 1 and 600 minutes (default 60 minutes) for the duration of the lease to the DHCP client.
- Check **Allow BOOTP clients** if you want the device DHCP server to respond to lease requests from BOOTP clients.



Note Do not check Allow BOOTP clients if some LAN devices use the BOOTP protocol to retrieve their operating system or firmware from a separate BOOTP server.

STEP 3 In the **DHCP Address Pool** table, configure IP address pool options:

- To use an IP address group, select **IP Address Group**. Then, select an existing group from the drop-down list
- To use a subnet, select **IP Subnet**. Then, type the subnet IP address and **Mask**.
- To use a range of IP addresses, select **IP Range**. Then, type begin and end of the address ranges.

STEP 4 To allow the device to provide the DHCP clients with different DNS server IP addresses than those configured on the device, check **Override Default DNS Settings**.

DNS settings are configured and managed from the **Network > Configuration > DNS** menu option.

STEP 5 Optionally, in the **WINS Servers** fields, type the IP addresses of up to two WINS servers for use by the client if you are using Windows networking.

STEP 6 Optionally, in the **NBX NCP** field, type the NBX network call processor (NCP) IP address if you want to allow NBX phones to retrieve the NCP IP address.

STEP 7 Click **Apply** to save the changes.



Note Ensure that the firewall rules configured on the device allow DHCP clients to send DHCP requests to the correct security zone and to receive their IP address by DHCP. For details, see [“Firewall” on page 63](#).

Disable the DHCP Server

STEP 1 From the LSM menu, select **Network > DHCP Server**. Then, click the **Configure DHCP** tab.

STEP 2 On the Configure DHCP Server page, clear the **Enable DHCP Server** checkbox.

DHCP Relay

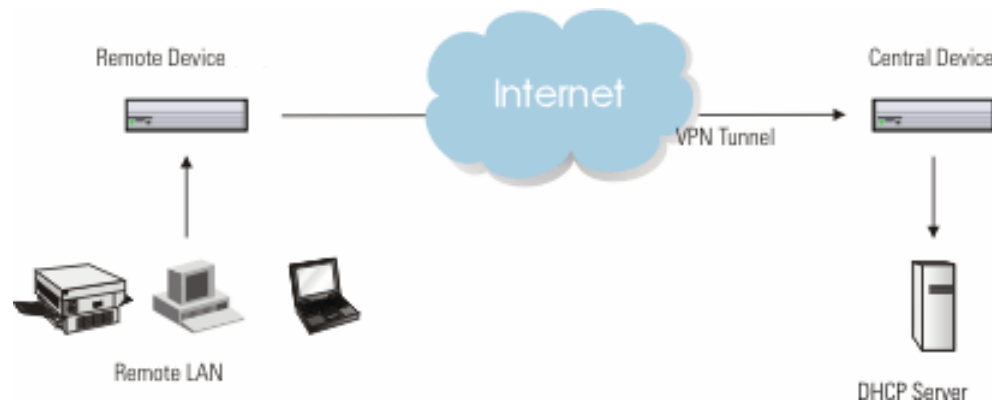


Note To use DHCP Relay, you must disable the DHCP Server. See [“Disable the DHCP Server” on page 170](#) for more information.

DHCP Relay allows DHCP to operate between a DHCP client on one security zone and a DHCP server on another. To use DHCP relay, you configure the device to act as a DHCP relay agent. The device will relay DHCP packets to the destination DHCP server and back to the client across security zone boundaries. This enables DHCP clients on different networks to use the same DHCP server.

You can configure the device to act as a central or remote relay agent as illustrated in the following figure:

Figure 6–14: DHCP Relay: Device Configuration for Central and Remote Agent



- A **Central Relay agent** is connected to the network that contains the DHCP server. It receives requests from a remote agent and forwards them to the DHCP server on its LAN. You can configure this option to work over VPN so that the device allows a DHCP server at one site to provide IP configuration to clients attached to a remote LAN. In this configuration, the device acts as a DHCP Relay agent and supports DHCP over VPN tunnels using IKE.
- A **Remote DHCP Relay Agent** is connected to a client network that requests a DHCP lease. It listens for DHCP requests from its LAN. When a client request is received, the agent inserts the Interface IP of the requestor into the DHCP request before it is relayed to the central DHCP server. This address, which is not contained in a DHCP address range, determines the scope of addresses used by the central DHCP server to allocate the address to the remote client.



Note For more detailed information on how DHCP Relay works, see the Concepts Guide.

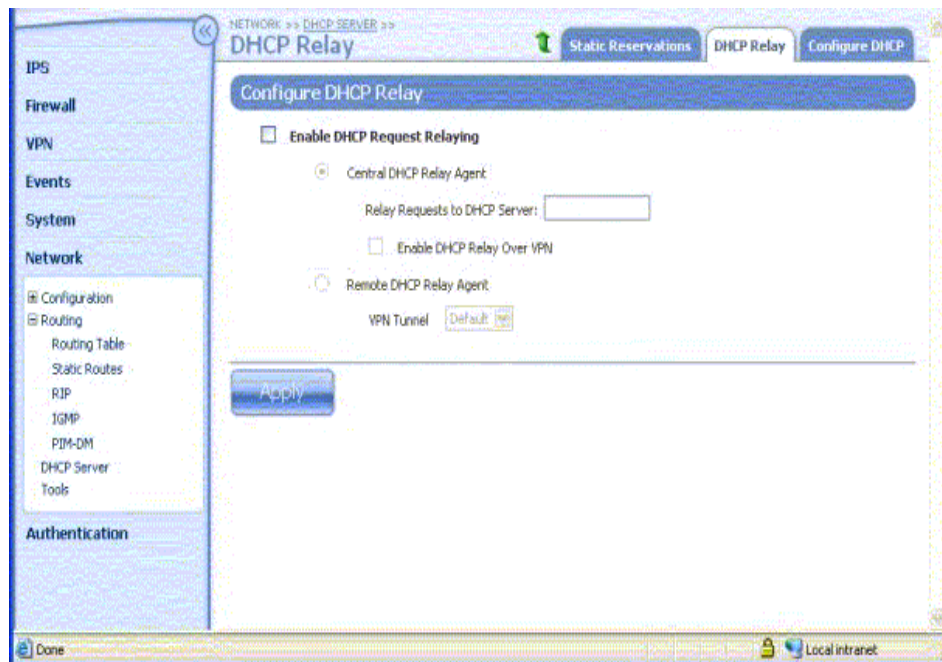
Configuring DHCP Relay

You can configure DHCP Relays from the DHCP Relay page (**Network > DHCP Server > DHCP Relay** tab). From this page, you can:

- Enable/disable the DHCP Relay option
- Configure the device as a Central DHCP agent with or without the Relay Over VPN option
- Configure the device as a Remote DHCP Relay Agent

The following figure shows the DHCP Relay page.

Figure 6–15: DHCP Server: DHCP Relay Page



The following table shows the configuration parameters to set up DHCP Relay

Table 6–5: Network: DHCP Relay Configuration Parameters

Parameter	Description
Enable DHCP Request Relaying	Select this option to enable DHCP Relay. You must disable the DHCP server before using this feature.
Central DHCP Relay Agent	Select this option if the device is directly connected to a network that contains the DHCP server (that is, the device is in the head office next to the DHCP Server). In this configuration, the device receives requests from remote agents (possibly X family devices) and forwards them to the DHCP server on its LAN.

Table 6–5: Network: DHCP Relay Configuration Parameters (Continued)

Parameter	Description
Relay Requests to DHCP Server	The IP address of the central DHCP server where requests are sent.
Enable DHCP Relay Over VPN	For a Central DHCP Relay Agent, selecting this checkbox allows the device to act as a VPN Relay agent and supports DHCP requests arriving over VPN tunnels using IKE. The device will forward the requests onto the DHCP server.
Remote DHCP Relay Agent	Select this option if the device is connected to a client network that sends DHCP lease requests. In this configuration, the device listens for DHCP requests from its LAN. This option is recommended for an device in a remote office that is relaying DHCP requests to a central DHCP server in the head office.
VPN Tunnel	If Remote DHCP Relay Agent is selected, this parameter identifies the VPN Tunnel the X family device uses to pass DHCP requests to the central DHCP relay agent.



Note If you are using **DHCP Relay over VPN**, any LAN devices attached to the Remote VPN Relay agent that are not using DHCP must be configured as Static Reservations. (See [“Static Reservations” on page 174](#)). To configure, navigate to **Network > DHCP Server**. Then, select the Static Reservations page.

You can only use DHCP Relay Over VPN when the VPN between two devices is configured to use Internet Key Exchange (IKE).

Configure DHCP Relay as a Central DHCP Relay in the Main Office

STEP 1 From the LSM menu, select **Network > DHCP Server**. Then, click the **DHCP Relay** tab.

STEP 2 On the DHCP Relay page, check **Enable DHCP Request Relaying** to enable DHCP Relay.

STEP 3 Select **Central DHCP Relay**.

With this configuration, the device is configured to receive requests from a remote agent which are then forwarded to the DHCP server on its LAN.

STEP 4 In the **Relay Requests to DHCP Server** field, type the address of the central DHCP server.

If you want the device to act as a **Central VPN Relay agent**, check **Enable DHCP Relay over VPN**.



Note Make sure that the tunnels connecting to device configured as the Remote VPN Relay agent are configured as **Destination network addresses assigned by DHCP** in the **Tunnel Setup** section of the VPN - Create Security IPSec Configuration page.

STEP 5 Click **Apply** to save the configuration.

Configure the DHCP Relay Mode as Remote VPN Relay Agent

STEP 1 From the LSM menu, select **Network > DHCP Server**. Then, click the **DHCP Relay** tab.

STEP 2 On the DHCP Relay page, check **Enable DHCP Request Relaying** to enable DHCP Relay.

STEP 3 Select **Remote DHCP Relay Agent**.

With this configuration, the device listens for DHCP requests from its LAN and forwards them to a Central DHCP Relay.

STEP 4 From the **VPN Tunnel** drop-down list, select the tunnel that will be used to relay the requests from the Remote DHCP Relay agent to the Central DHCP Relay agent.



Note If the VPN Tunnel list is empty, navigate to **VPN > IPSec/IKE Status** and configure an IPSec tunnel.

STEP 5 Click **Apply** to save the configuration.

Static Reservations

Static Reservations allow you to assign a particular IP address to a device such as a printer or DNS server. In the LSM, you can create and manage static reservations from the Static Reservations page (**Network > DHCP Server**). From this page, you can complete the following tasks:

- View a list of current static reservations
- Create a new reservation
- Delete a reservation




Note If you are using [DHCP Relay](#), any LAN devices attached to the Remote VPN Relay agent that are not using DHCP must be configured as static mappings.

The following figure shows the DHCP Static Reservations page:

Figure 6–16: Network: DHCP Static Reservations Page

The **Current Reservations** table provides the following information for each static reservation:

Table 6–6: Static Reservation Details

Column	Description
IP Address	The IP address you want to assign to the device
MAC Address	The MAC address of the device
Function(s): 	The available functions for static reservations: <ul style="list-style-type: none"> Delete a static reservation.

Add a Static Reservation

- STEP 1** From the LSM menu, select **Network > DHCP Server**. Then, click the **Static Reservations** tab.
- STEP 2** On the Static Reservations page, type the **IP address** you want to assign to the device.
- STEP 3** Type the **MAC Address** for the device.
- STEP 4** Click **Add to table below** to update the **Current Reservations** table.

Continue to add reservations to the table as required, following steps 2 to 4.

For information on the maximum number of reservations your device supports, see “[Appendix D, “Device Maximum Values.”](#)”

[DHCP Server](#)

Network Tools

The LSM provides the following network tools:

- **DNS Lookup** — a network tool that displays the IP Address for a given DNS name
- **Find Outgoing zone**— a network tool that displays the physical interface/security zone (and router IP address if appropriate) that the device would use to reach a given location
- **Traffic Capture** — a network tool that allows you to capture network packets into a file. This is useful for analyzing the type of traffic flowing through the device
- **Ping** — a network tool that allows you to send out Ping requests to test whether devices on an IP network are accessible and functioning correctly. This feature helps diagnose connectivity problems such as a failed network device between the device and the web server being accessed, or to help diagnose DNS setup problems
- **Traceroute** — a network tool that allows you to display the network hops from the device to another device on an IP network. This is a useful tool for network troubleshooting

For additional information, see the following topics:

- [“DNS Lookup” on page 177](#)
- [“Traffic Capture” on page 177](#)
- [“Find Network Path” on page 177](#)
- [“Ping” on page 178](#)
- [“Traceroute” on page 179](#)

DNS Lookup

Use the DNS Lookup tool to find the IP address for a given DNS name. DNS lookup can be used to verify that the DNS Servers on the device are configured properly.

Find the IP address for a DNS name

STEP 1 From the LSM, select **Network > Tools**.

STEP 2 In the **DNS Lookup** table, type the **Hostname** in the **IP** field.

STEP 3 Click **DNS Lookup**.

The IP addresses and aliases associated with the DNS name are displayed.

Find Network Path

Use the **Find Network Path** tool to display the security zone or tunnel name (and router IP address if appropriate) that the device would use to reach a given location.

Find an Outgoing Zone

STEP 1 From the LSM, select **Network > Tools**.

STEP 2 On the Tools page in the **Find Network Path** table, type the **Hostname** or **IP address** of the device to which you want to find the network path.

STEP 3 Click **Find**.

The Find Network Path page displays showing the name of the security zone or tunnel the device uses to contact the specified destination. If the device cannot resolve the specified destination, `Unknown host` displays.

The device uses the routing table to determine where to send a packet destined for this address, and displays the routing path information such as security zone or tunnel name. If the device cannot resolve the specified destination, `Unknown host` displays.

Traffic Capture

Use the **Traffic Capture** tool to capture network packets in a file. This is useful for analyzing the type of traffic flowing through the device.

From the Traffic Capture page, you can:

- View and manage existing packet capture files.
To view and manage packet capture files, select **Network > Tools > Traffic Capture**. Then, select the **Traffic Capture** tab.
- Create a new traffic capture file. To see a list of packet capture files, go to **Network > Tools > Traffic Capture**.

Perform a Traffic Capture

- STEP 1** From the LSM, select **Network > Tools**. On the Tools page, click the **Traffic Capture** tab.
- STEP 2** On the Traffic Capture page, click **Create Capture File**.
- STEP 3** On the Create Traffic Capture page, specify the Capture File Details:
- STEP A** If required, change the settings for the **Max File Size** (upper limit is 10000000) and the **Max Packets** (upper limit is 10000).
- STEP B** Select the security **Zone Pair** on which you want to capture traffic.
- STEP 4** Optionally, to further specify which packets to include in the capture, enter IP protocol and source/destination addresses parameters in the **Capture Filter** table.
- STEP 5** Click **Start Capture**.

Ping

Use the **Ping** feature to send Ping requests to test whether devices on an IP network are accessible and functioning correctly.

Ping can help diagnose connectivity problems such as a failed network device between the device and the web server being accessed, or to help diagnose DNS setup problems. For example, if the device cannot access *www.mycompany.com*, enter *www.mycompany.com* in the **Host IP** field and click **Start Ping**. If the IP address for the Host appears in the **Output** table, the DNS server can be contacted and is working correctly. The problem is therefore a connectivity issue between the device and the original web server.



Note Ensure that the policies configured on the device allow the security zone to send Ping (ICMP) requests. A firewall rule allowing Ping requests between zones allows the request to be sent to the destination zone and the response to be allowed back to the source zone.

Ping a device

- STEP 1** From the LSM menu, select **Network > Tools**.
- STEP 2** On the Tools page, click the **Ping** tab.
- STEP 3** On the Ping page in the **Ping Configuration** table, type the **Host Name** or **IP** address for the device that you want to ping.

STEP 4 If required, configure any of the following options:

- **Inter Packet Interval** — the number of seconds between each packet
- **TTL** — (IP Time To Live) the maximum number of IP routers that the packet can go through before being thrown away. Each router will decrease the TTL value on the packet by one. The maximum value is 255
- **Number Of Packets** — the number of packets you want to send
- **Silent** — do not display any extra information
- **Perform Reverse Lookup on Results** — If you locate a domain name, this function returns the IP address. if you have located an IP address, this returns the domain name.
- **Record Route** — the route the packet took through the network/Internet. Some routers will add their address to the packet if you check this option
- **Verbose** — more details about the ping will be displayed if you check this option



Note To reset the Ping Configuration default values, click **Defaults**.

STEP 5 Click **Start Ping**.

STEP 6 The device sends a Ping request to the specified device.

If the device is accessible and functioning correctly, a message similar to the following is displayed:

```
64 bytes from 192.168.1.254: icmp_seq=0 ttl=248 time=195.2 ms
```

If the device is not accessible, or is not functioning correctly, a message similar to the following is displayed:

```
No answer from 192.168.1.254
```

Some network environments block Ping traffic on the network. The Ping request may therefore fail even if the network device is operating normally.

Traceroute

Use the **Traceroute** tool to display the network hops from the device to another device on an IP network. This feature is useful to diagnose connectivity problems such as a failed network device between the device and the web server being accessed.

Perform a Traceroute

STEP 1 From the LSM menu, select **Network > Tools**.

STEP 2 On the Tools page, click the **Traceroute** tab.

STEP 3 On the Traceroute page in the **Traceroute Configuration** table, type the **Host Name** or **IP address** of the destination device to which you want to trace the route.

STEP 4 Configure any of the following options:

- **First Hop** — you can choose which is the first hop that you get information about. For example, if you already know about the first four hops, enter 5
- **Probe Type** — select the communications protocol or the traceroute: UDP or ICMP
- **Max Hops** — the maximum number of hops for the traceroute
- **Print Name** — whether or not you want the trace route to query and display the DNS names of the routers
- **Port Base** — the port number from which the packet is sent. Leave as default value
- **Max Number of Timeouts** — the maximum number of timeouts after which the traceroute stops
- **Number Of Queries** — the number of packets that will be sent to each hop
- **Max Wait** — the maximum time in milliseconds the traceroute will wait for a response from the destination host before stopping
- **Calculate Checksum** — whether or not to use checksums

STEP 5 Click **Start Traceroute**.

The device sends a trace route request to the specified device and a message similar to the following is displayed:

```
traceroute to 192.168.1.251, 30 hops max, 38 byte packets
```

If the device is accessible and functioning correctly, a message similar to the following is displayed which displays the network hops. Each hop may take a few seconds to complete:

```
1.router1 (192.168.1.252) 1.292ms, 1.343ms, 1.810ms
2.router2 (192.168.1.253) 26.027ms, 27.156ms, 44.902ms
3.router3 (192.168.1.254) 24.323ms, 24.854ms, 30.096ms
4.router4 (192.168.1.255) 27.303ms, 33.639ms
```

If the device is not accessible, or is not functioning correctly, only the hops that worked are displayed.



Note Some network environments block trace route traffic on the network. The TraceRoute request may therefore fail even if the network device is operating normally.

7 VPN

The VPN section provides an overview of Virtual Private Networks and describes how they are implemented.

Overview

The VPN menu pages in the LSM allow you to configure the protocol and authentication method for VPN tunnels so that remote users and devices can access the X family device. The following menu options are available:

- **IPSec Status** — View and manage IPSec configuration for the X family device. This page also provides access to the IPSec Configuration page to enable and configure IPSec and to manage the IPSec Security Associations. Use this option when you are configuring a site-to-site VPN connection, or a client-to-site connection that relies on the IPSec or L2TP over IPSec tunneling protocol.
- **IKE Proposal** — View, set up, and/or modify configuration for IKE phase 1 and phase 2. Use this option if you want to use IKE as the keying mode to negotiate an IPSec or L2TP over IPSec VPN connection.
- **L2TP Status** — View current L2TP connections, configure the X family device to act as an L2TP server. Use this option for client-to-site connections that use L2TP or L2TP over IPSec.
- **PPTP Status** — View current PPTP connections, configure the X family device to act as a PPTP server. Use this option for client-to-site connections to support remote users. The PPTP protocol is the least secure method for VPN connections.

Before using the available menu options, review the VPN chapter in the *Concepts Guide*.

For additional information, see the following topics:

- [“About VPN” on page 182](#)
- [“IPSec Configuration” on page 184](#)
- [“IKE Proposal” on page 198](#)
- [“L2TP Configuration” on page 208](#)
- [“PPTP Configuration” on page 212](#)

About VPN

A **Virtual Private Network (VPN)** uses a public network infrastructure such as the Internet to link physically separate private networks together to form one large virtual private network. The data is kept private by using encryption.

A VPN uses packet encryption to tunnel across the public connection from the Initiation Point to the Termination Point.

- **Initiation** occurs when the user or device requests access to the remote company LAN. Tunnel initiation is usually accomplished using VPN client software on a PC, or through VPN support in an access router or Firewall, such as the X family.
- **Termination** refers to the point in the network at which the identity of the remote party is validated, the VPN tunnel is created, and the remote party enters the network. VPN termination is typically supported in routers, secure gateways, Internet Firewalls, or in software residing on a network server.

In general, for the purpose of configuration, VPNs can be broadly grouped into two main types:

- **Site-to-site.** A VPN tunnel established between two X family devices, typically used for office-to-office connectivity.
- **Client-to-site.** A VPN tunnel established between the X family and a VPN client application, typically used to connect off-site users to an office network.

VPN Connection Security Features

The X family uses three main security features to ensure the secure VPN connections: tunneling, authentication, and encryption. These features work together to protect network resources and guarantee secure private connections across the public network.

- **Tunneling** describes the link created between two endpoints in a VPN connection — for instance between an employee’s home-office computer and the company network. Tunneling ensures that data exchanged across the link is encapsulated, or wrapped in protocols and data encryption methods which prevent unauthorized users from intercepting or corrupting the data. The X family provides three tunneling protocols to support VPN capabilities:
 - IPSec
 - L2TP over IPSec (recommended) or L2TP
 - PPTP

- **Authentication** establishes the identity of a remote user or device to verify that they have permission to access network resources. The X family provides two types of authentication methods:
 - *User Authentication* — username/password verification methods to ensure that only authorized users may access client-to-site VPNs. Access privileges are used to control what network services are available to each user. On the X family device, user accounts are configured from the Authentication menu page. L2TP over IPSec and PPTP VPN protocols use user authentication.
 - *Packet Authentication* — provides data integrity and origin authentication while also providing protection against replay attacks. The X family device supports PKI (Public Key Infrastructure) for IPSec with X.509 certificates.
- **Encryption** is applied to the tunneled connection to scramble data, thus making data legible only to recipients with the correct key. Using cryptographic algorithms, information is scrambled (encrypted) by the initiator and then unscrambled (decrypted) when it reaches the recipient. Recipients of encrypted data must have access privileges and hold specific keys in order to read the data.



Note This user guide describes the LSM menu pages and parameters available for VPN configuration and management. It also provides procedures to configure tunneling protocols and IKE proposals. For a more detailed explanation of VPN Configuration along with deployment scenarios, see the Concepts Guide, available from the X family product documentation section of the TMC website.

For additional information, see the following topics:

- [“VPN Configuration Overview” on page 183](#)
- [“IKE Proposal” on page 198](#)
- [“IPSec Configuration” on page 184](#)
- [“L2TP Configuration” on page 208](#)
- [“PPTP Configuration” on page 212](#)

VPN Configuration Overview



Note This user guide describes the LSM menu pages and parameters available for VPN configuration and management. It also provides procedures to configure tunneling protocols and IKE proposals. For a broader explanation of VPN Configuration along with deployment scenarios, see the Concepts Guide.

Use the following overview to guide the VPN Setup process for the X family device:

- STEP 1** Install the high-encryption service pack on the device.

By default all new X family devices are supplied with 56-bit DES encryption only. To enable the strong encryption functionality (3DES, 128-AES, 192-AES, 256-AES) required to create secure VPN connections, install the correct Strong Encryption Service Pack for your device available from the TMC Web site.

- STEP 2** Decide whether you require a site-to-site or client-to-site VPN connection.

- STEP 3** For client-to-site VPNs, determine whether you will use the PPTP, L2TP, or L2TP over IPSec tunneling protocol. PPTP and L2TP are not recommended because they are not very secure.
- For site-to-site VPN connections, you must use the IPSec protocol. For authentication, you can use either X.509 certificates or Pre-Shared Key (PSK). X.509 certificates are recommended because they are more secure.
- STEP 4** If you are using PPTP or L2TP, configure the User Accounts, Privilege groups, and RADIUS Server settings for user authentication. Then, configure the PPTP or L2TP VPN tunnel. For details, see [“Enable PPTP Server and Configure PPTP Client and Addresses” on page 215](#) and [“Enable L2TP Server and Configure L2TP Client and Addresses” on page 211](#).
- If you are using L2TP over IPSec or IPSec with X.509 Certificates for authentication as recommended, configure the certificates. For details, see [“X.509 Certificates” on page 255](#).
- STEP 5** For IPSec or L2TP over IPSec, configure the IKE proposals that can be used to encrypt and authenticate VPN tunnel connections. You will use the proposal when you configure the IPSec Security Association for each remote site. To simplify configuration for client-to-site (L2TP over IPSec) and site-to-site VPN connections, you can edit the default IKE proposal pre-configured on the X family device.
- STEP 6** For site-to-site connections, if the VPN traffic will come from multiple subnets or go to multiple subnets, configure IP address groups with the subnets that will be used. For details, see [“IP Addresses: Configuration Overview” on page 142](#).
- STEP 7** Enable IPSec and configure the Security Associations that setup authentication and determine what traffic is allowed over the VPN connection.
- For site-to-site configuration, see [“Configure an IPSec SA for a Site-to-Site VPN Connection” on page 195](#). You must configure a separate Security Association for each remote site.
- For client-to-site configuration using L2TP over IPSec, use the default SA pre-configured on the device. For details, see [“Edit the Default SA for Client-to-Site VPN Connections using L2TP over IPSec” on page 194](#).

IPSec Configuration

IPSec is a security protocol that can be used to secure IP traffic between two remote private networks connected through a public network. It is a flexible protocol with a wide range of encryption options. IPSec is commonly used for both site-to-site connections between separate private networks (tunnels) and for client-to-site connections between remote PCs and private networks. IPSec is the standard X family method of setting up a network-to-network VPN connection.



Note You must enable IPSec globally in order to use it for IPSec VPNs.

To use the IPSec protocol, you need to configure an **IPSec Security Association (IPSec SA)** which consists of configuration parameters that allow two devices to establish an IPSec tunnel for secure communication across a public network.

You can view and manage IPSec configuration from the IPSec Status page (**VPN > IPSec Status**).

The following figure shows the IPSec Status page:

Figure 7–1: IPSec Status Page

Name	Peer IP Address	Local ID	Peer ID	Proposal	Status	Function(s)
Default	0.0.0.0	10.171.2.254	0.0.0.0	DES_CBC-SHA1-OH1	Phase 1: Idle	
Default	152.67.137.49	10.100.71.100	152.67.137.49	ESP DES-CBC-ESP SHA-1 HMAC-No PFS	Phase 2: Established	

From this page, you can complete the following tasks:

- If IPSec is enabled, view current status of the IPSec SA Phase 1 and Phase 2 negotiation process.
- View a summary of IPSec SA that have been used to negotiate tunnels on the device.
- Renegotiate IKE Phase 1 or Phase 2 of the IPSec VPN connection.
- Access the IPSec Configuration page to enable IPSec and view and manage the IPSec Security Associations required to establish a VPN connection.

For additional information, see the following topics:

- [“IPSec Status Details” on page 185](#)
- [“IPSec Configuration” on page 187](#)


IPSec Status Details

If IPSec is enabled, the **IPSec Status** table provides information about the IPSec Security Associations currently configured on the X family device:

Table 7–1: IPSec Status Details

Column	Description
Name	The name of the security association that is configured for this connection. The Default SA is a pre-installed SA used if no other SA matches the VPN connection
Peer IP Address	The public IP address of the remote VPN X family or network device
Local ID	The Local ID information used to negotiate IKE Phase 1.
Peer ID	The Peer ID information used to negotiate IKE Phase 1.
Proposal	The IKE proposal used to negotiate the VPN connection.

Table 7–1: IPSec Status Details (Continued)

Column	Description
Status	<p>The current status of the connection:</p> <p>Phase 1: Idle — Phase 1 negotiation has not started, or it has started but the connection subsequently timed out, or did not complete successfully</p> <p>Phase 1: Negotiating — the X family device is in the process of authenticating a Phase 1 of the IPSec VPN connection</p> <p>Phase 1: Failed — the negotiation failed</p> <p>Phase 1: Established — the X family device has successfully completed Phase 1 negotiation.</p> <p>Phase 2: Idle — Phase 2 negotiation has not started, or it has started but the connection subsequently timed out, or did not complete successfully</p> <p>Phase 2: Negotiating — the X family device is in the process of establishing a Phase 2 of the IPSec VPN connection.</p> <p>Phase 2: Established — a remote device is successfully connected</p> <p>Phase 2: Failed — the negotiation failed</p> <p>Note If you have selected the Enable Verbose messages in the VPN Log option in the IPSec Configuration, you can view more detailed information on the status of the Phase 1 and Phase 2 negotiation in the VPN Log (Events > Logs > VPN Log).</p>
Function(s) 	<p>The functions available to manage the IPSec SA VPN connection:</p> <ul style="list-style-type: none"> Renegotiate a Phase 1 or Phase 2 connection for the IPSec SA.

IPSec Configuration

Use the IPSec Configuration page (VPN > **IPSec Status, IPSec Configuration tab**) to view and manage the IPSec configuration and the IPSec Security Associations. IPSec configuration is required if you want to use site-to-site or client-to-site L2TP over IPSec VPN tunnels.

The following figure shows the IPSec Configuration page:

Figure 7–2: VPN: IPSec Configuration Page

VPN >> IPSEC STATUS >> **IPSec Configuration** ↑ IPSec Configuration

IPSec Global Setup

☒ Enable Verbose messages in the VPN Log

☒ Enable IPSec Global VPNs

Local Domain Name

Local Email Address

IP Security Associations

25 Records per page

Name	Keying Mode	IPSec Gateway	Local Network(s)	Remote Network(s)	Function(s)
Default	IKE-PSK(DES-SHA1-PSK)	-	-	-	

You can complete the following tasks from this page:

- Enable IPSec Global VPNs on the X family device
- Configure the Local ID Domain Name and Email address used to negotiate IKE proposals
- View current IP Security Associations configured on the X family device
- Create/Edit Security Associations used to establish VPN tunnel connections



For additional information, see the following topics:

- [“IPSec Configuration Parameters and IP Security Association Details” on page 188](#)
- [“Enable and Configure IPSec Global Settings” on page 189](#)
- [“Configure an IPSec Security Association” on page 189](#)
- [“Edit the Default SA for Client-to-Site VPN Connections using L2TP over IPSec” on page 194](#)

IPSec Configuration Parameters and IP Security Association Details

The following table describes the configuration parameters for the IPSec security protocol:

Table 7–2: IPSec Configuration Parameters and IP Security Association Details

Parameter	Description
IPSec Global Setup	
Enable Verbose messages in the VPN Log	Select this option to log more detailed information when the X family device is establishing a VPN connection.
Enable IPSec Global VPNs	Check this option to enable IPSec globally on the X family device.
Local Domain Name	Enter the Domain Name for the Local ID. If specified, this value can be used to authenticate Phase 1 of the IKE proposal. You only need to specify this parameter if the IKE proposal is configured for aggressive mode.
Local Email Address	Enter the Email address to use for the Local ID. If specified, this value can be used to authenticate Phase 1 of the IKE proposal. You only need to specify this parameter if the IKE proposal is configured for aggressive mode.
IP Security Association Details: This table displays the IPSec Security Associations (SAs) that have been configured on the X family device.	
Name	The name of the IPSec Security Association.
Keying Mode	Shows the Keying mode configured for the IPSec Security Association. For additional information on keying modes, see “Configure an IPSec SA for a Site-to-Site VPN Connection” on page 195 and “Edit the Default SA for Client-to-Site VPN Connections using L2TP over IPSec” on page 194 .
IPSec Gateway	The IP address of the peer VPN device
Local Network	Shows what local traffic may access or be accessed over the VPN based on the SA configuration.
Remote Network	Shows what traffic can be sent over the VPN tunnel based on the SA configuration.
Functions	Icons representing functions to manage the IPSec Security Associations. The following functions are available: <div style="display: flex; align-items: center;">  <ul style="list-style-type: none"> • Delete an SA </div> <p>Note You cannot delete the default SA.</p> <div style="display: flex; align-items: center;">  <ul style="list-style-type: none"> • Edit an SA </div>

Enable and Configure IPSec Global Settings



Note Before configuring IPSec and the IPSec Security Association, configure the required IP Address Groups and the IKE proposals. For details, see [“Configuring IKE Proposals” on page 200](#).

- STEP 1** From the LSM menu, select **VPN > IPSec Status**. Then, click the **IPSec Configuration** tab.
- STEP 2** On the IPSec Configuration page, check **Enable IPSec Global VPNs**.
- STEP 3** Check **Enable Verbose messages in the VPN log** to generate more detailed information on the VPN connection process.
- This option is only recommended if you need to troubleshoot problems with the VPN tunnel connection.
- STEP 4** Type a **Local Domain Name** and **Local Email Address** for the X family device.
- The values specified define the Local ID for the device which can be used to authenticate Phase 1 of the IKE proposal. You only need to complete these fields if the authentication type for the IKE proposal used by the SA is configured for aggressive mode.
- STEP 5** Click **Apply**.

After configuring IPSec, you need to create the Security Association that allows two devices to establish the secure IPSec tunnel for the VPN connection. You can edit the Default Security Association, or create a new one.

For details, see [“Configure an IPSec Security Association” on page 189](#).

Configure an IPSec Security Association

An IPSec Security Association (IPSec SA) consists of configuration parameters that allow two devices to establish an IPSec tunnel. On the X family device, you need to configure an IPSec Security Association that allows the device to connect to the remote network (site-to-site) or device (client-to-site)

The device provides a Default Security Association (**Default**) mainly for Client-to-Site VPNs.

- The Default SA is typically used for the deployment of multiple VPN clients. All the clients can use this default SA, instead of creating one SA per client. The Default SA is for incoming connections only, and is used if the device cannot match the IKE identification to any other SA.
- The Default SA can also be used to terminate incoming VPN site-to-site connections if the **Enable IPSec Tunnel connections** option is selected.



Note You cannot delete the Default SA and you cannot edit the Default SA Name, Peer IP Address or Keying Mode.

If you want the device to initiate the VPN connection for a site-to-site connection, you must create a unique security association for each site-to-site VPN connection

The following is an overview of the Security Association configuration process.

- STEP 1 IPSec Security Association Setup** — configure the Peer ID address, terminated security zone, and keying mode
- STEP 2** Select the **Keying Mode**, either IKE or Manual.
Manual keying is only recommended for testing as this mode is not secure.
- STEP 3** Set up the keys used to authenticate the VPN connection. Depending on the keying mode selected, specify the parameters for **IKE Setup** or **Manual Setup**.
- STEP 4 Tunnel Setup**—select the method to route VPN traffic on the local and remote networks. In this step, you can also enable NAT if you want to perform NAT on traffic entering a VPN tunnel, or configure a VPN Supernet for a hub-and-spoke network (for details, see the *Concepts Guide*.)

For additional information on IPSec SA Configuration, see the following topics:

- [“IPSec Security Association Configuration Parameters” on page 190](#)
- [“Edit the Default SA for Client-to-Site VPN Connections using L2TP over IPSec” on page 194](#)
- [“Configure an IPSec SA for a Site-to-Site VPN Connection” on page 195](#)
- [“Edit the Default SA for Site-to-Site VPN Connections” on page 197](#)

IPSec Security Association Configuration Parameters

The following table describes the IPSec SA configuration parameters. To review the parameter descriptions for a particular group of settings, see the following links:

- [“IPSec Security Association Setup” on page 190](#)
- [“Keying Mode” on page 191](#)
- [“IKE Setup:” on page 191](#)
- [“Manual Setup:” on page 192](#)
- [“Tunnel Setup” on page 193](#)

Table 7–3: IPSec Security Association Configuration Parameters

Parameter	Description
IPSec Security Association Setup	
Name	Enter the name for the Security Association. When a VPN connection is established using IPSec, this name identifies the SA used to make the connection on the IPSec Status page.
Peer IP Address	Enter the IP address of the terminating X family or other network device (the target of the VPN link). Note If you set this to 0.0.0.0, the IPSec can only terminate VPNs.

Table 7-3: IPSec Security Association Configuration Parameters (Continued)

Parameter	Description
Terminated Security Zone	<p>Select the remote security zone on which to terminate the VPN from the Terminated Security Zone drop-down list.</p> <p>All devices within the termination zone have unrestricted access to the VPN. Traffic received over the VPN has unrestricted access to all devices within the termination zone. Firewall rules must be used to access other zones.</p> <p>To use NAT within a VPN tunnel, you must select a virtual security zone (such as the VPN default security zone) that contains no physical ports.</p>
Keying Mode	<p>Select the method to use for authenticating access to the VPN from the Keying Mode drop-down list, either:</p> <ul style="list-style-type: none"> • IKE — provides more security than manual keying. If this option is selected, the IKE Setup table displays the IKE parameters. • Manual — provides the lowest level of security. If this option is selected, the Manual Setup table displays the Manual Key parameters.
Enable Security Association	Check this box to enable the Security Association so that it can be used to establish VPN connections.
Support GRE and L2TP	Check this box to use this Security Association for L2TP or GRE VPNs. Both tunneling protocols can use IPSec to authenticate and encrypt the connection.
IKE Setup: These configuration options are available if IKE is selected as the Keying mode.	
IKE Proposal	Select the IKE proposal the X family device will use to authenticate VPN connections from the drop-down list. IKE Proposals are setup from the IKE Proposal page (VPN > IKE Proposal).
Shared Secret	If you selected an IKE proposal that authenticates with a Pre-shared Key (PSK), enter the Pre-Shared Key used to validate access to the VPN.
Peer Email Address	If the selected IKE proposal uses Email Address for the Peer ID, enter the Email Address that the X family device will use to authenticate Phase 1 of the IKE proposal.
Peer Domain Name	If the selected IKE proposal uses Domain Name for the Peer ID, enter the Domain Name for the Peer ID that the X family device will use to authenticate Phase 1 of the IKE proposal.
Peer Distinguished Name	If the selected IKE proposal uses <i>Distinguished Name</i> for the Peer ID, enter the Domain Name that the X family device will use to authenticate Phase 1 of the IKE proposal.

Table 7–3: IPSec Security Association Configuration Parameters (Continued)

Parameter	Description
Manual Setup: These configuration parameters are available if Manual is selected as the Keying mode.	
Encryption	Select an appropriate encryption method: <ul style="list-style-type: none"> • ESP DES-CBC (weak encryption, not recommended) • ESP 3DES-CBC (strong encryption) • ESP AES-CBC-128 (strong encryption) • ESP AES-CBC-192 (strong encryption) • ESP AES-CBC-256 (strong encryption) Enter a hexadecimal Key value for the key. Note By default all new X family devices are supplied with 56-bit DES encryption only. To enable the strong encryption functionality (3DES, 128-AES, 192-AES, 256-AES) required to create secure VPN connections, install the correct Strong Encryption Service Pack for your device available from the TMC Web site.
Authentication	Select an appropriate authentication method: <ul style="list-style-type: none"> • ESP MD5 HMAC • ESP SHA-1 HMAC (recommended) • AH MDS • AH SHA-1 Enter a hexadecimal Key value for the key.
Incoming SPI (hex) Outgoing SPI (hex)	In the Incoming SPI (hex) and Outgoing SPI (hex) fields respectively, enter unique hexadecimal values (from 1 to 8 characters) for the incoming and outgoing SPI. When you configure the remote device, specify the same SPI values in reverse order. That is, use the incoming SPI value specified here as the outgoing SPI on the remote device. Use the outgoing SPI value specified here as the incoming SPI on the remote device. The Security Parameter Index (SPI) identifies the cryptographic keys and algorithms to be used to establish a VPN tunnel. For additional information, see the <i>Concepts Guide</i> .

Table 7–3: IPSec Security Association Configuration Parameters (Continued)

Parameter	Description
Tunnel Setup	
Local Networks	<p>Select one of the following methods to determine what local traffic may access or be accessed from the VPN tunnel. This method is only used for IPSec tunnel mode connections:</p> <ul style="list-style-type: none"> • IP Address Group (configure from Network > Configuration > IP Address Groups) - use this option if traffic allowed over the VPN tunnel is from multiple IP subnets. • IP Subnet • IP Range • Peer uses tunnel as default route <p>Select this method if you have want the IPSec tunnel to be used as the default route for the device.</p> <ul style="list-style-type: none"> • Local addresses assigned by DHCP through this tunnel <p>Select this method if the connection will be used to connect two X family devices that have been configured to use <i>DHCP Relay over VPN</i>.</p>
Remote Networks	<p>Select one of the following methods to determine what traffic should be routed over the VPN tunnel. This method is only used for IPSec tunnel mode connections:</p> <ul style="list-style-type: none"> • IP Address Group (configure from Network > Configuration > IP Address Groups) - use this option if traffic allowed over the VPN tunnel is from multiple IP subnets. • IP Subnet • IP Range • Peer uses tunnel as default route <p>Select this method if you have want the IPSec tunnel to be used as the default route for the device.</p> <ul style="list-style-type: none"> • Local addresses assigned by DHCP through this tunnel <p>Select this method if the connection will be used to connect two X family devices that have been configured to use <i>DHCP Relay over VPN</i>.</p>

Table 7-3: IPSec Security Association Configuration Parameters (Continued)

Parameter	Description
Enable NAT of local network addresses	<p>Enable this option to perform NAT on traffic entering a VPN tunnel. Selecting this option allows multiple remote VPN sites can use the same IP subnet.</p> <p>If you enable NAT, enter the NAT IP Address. This address must be included in the Local ID configured for the local network.</p> <p>Only one NAT IP address can be used for outgoing sessions for one VPN tunnel. However, you can configure an <i>all-services</i> Virtual Server for other specific IP addresses. These servers will use the virtual server public IP address for outgoing sessions when VPN NAT is enabled. This provides one-to-one NAT capability within VPN tunnels. For details, see “Configuring Virtual Servers” on page 84.</p> <p>If you enable NAT for the VPN tunnel, the <i>Terminated Security Zone</i> configured for the Security Association must be virtual, no physical ports assigned to the zone.</p>

For details on configuring IPSec Security Associations, see the following topics:

- [“IPSec Security Association Configuration Parameters” on page 190](#)
- [“Edit the Default SA for Client-to-Site VPN Connections using L2TP over IPSec” on page 194](#)
- [“Edit the Default SA for Site-to-Site VPN Connections” on page 197](#)
- [“Configure an IPSec SA for a Site-to-Site VPN Connection” on page 195](#)

Edit the Default SA for Client-to-Site VPN Connections using L2TP over IPSec

- STEP 1** From the LSM menu, select **VPN > IPSec Status**. Then, select the **IPSec Configuration** tab. The VPN - IP Security/ IKE page displays.
- STEP 2** On the IPSec Configuration page in the IP Security Associations table, click the **Pencil** icon to for the **Default** SA entry.
- STEP 3** On the Edit IP Security Association page, in the IP Security Association Setup table, check **Enable Security Association** to enable the Default SA.
- STEP 4** To enable the X family device to use the Default SA for L2TP VPNs, check **Support L2TP**. L2TP uses IPSec transport mode.
- STEP 5** For **IKE Setup**, select the **IKE Proposal** from the drop-down list of proposals currently configured.
- STEP 6** If you have selected an IKE Proposal with pre-shared key (PSK), type the **Shared Secret**. The same pre-shared key or X.509 Certificate must be available on the remote device establishing a VPN tunnel with the local device.

STEP 7 Click **Save** to save the configuration.

Click **Cancel** to return to the IPSec Configuration page without saving the changes.

All devices within the termination zone have unrestricted access to the VPN. Traffic received over the VPN has unrestricted access to all devices within the termination zone. Firewall rules must be configured to access the other zones.

Configure an IPSec SA for a Site-to-Site VPN Connection

If you want the X family device to initiate the connection, you must configure a unique security association for each site-to-site VPN connection.

STEP 1 From the LSM menu, select **VPN > IPSec Status**. Then, select the IP Configuration tab.

STEP 2 On the IPSec Configuration page, click **Create**, or to edit an existing security association, click its **Pencil** icon.

STEP 3 On the Create/Edit IP Security Association page, type or edit the name for the security association in the **Name** field.

Choose a name that helps you identify the link for which you are creating the security association.

STEP 4 In the **Peer IP Address** field, type the public IP address of the terminating VPN X family or network device (the remote target of the VPN link).



Note If you set this to 0.0.0.0, the IPSec SA can only terminate VPNs.

STEP 5 Select the security zone on which to terminate the VPN from the **Terminated Security Zone** drop-down list.

If you want to enable NAT for the VPN tunnel, select a virtual security zone (such as the VPN default security zone) that contains no physical ports.

STEP 6 Check **Enable Security Association** to enable this security association.

STEP 7 For GRE and L2TP over IPSec VPN tunnels, check **Support GRE and L2TP**.

STEP 8 Select the method to obtain authentication keys from the **Keying Mode** drop-down list, either:

- **IKE** — automatically generates keys periodically which provides more security than manual keying
- **Manual** — uses the fixed keys configured for the SA. This method provides the lowest level of security and is not recommended.

STEP 9 Configure the key information based on the Keying Mode selected.

- For **IKE Setup**, select the **IKE Proposal** from the drop-down list of proposals currently configured and then:
 - o For **IKE with PSK (Main Mode and Aggressive Mode)**, enter the Pre-shared Key (between 8 and 128 characters) used to validate access to the VPN in the **Shared Secret** field.

The same pre-shared key must be configured on the remote device establishing a VPN tunnel with the local device.

- o Additionally, for **IKE with PSK (Aggressive Mode only)**, enter the Peer (remote) ID you want to use in the appropriate field, either **Peer Email Address** or **Peer Domain Name**, depending on the **Peer ID Type** specified for the IKE Proposal (VPN > IKE Proposal).
If you specified **IP Address** as the **Peer ID Type** in the IKE Proposal page, the address you entered in the **Peer IP Address** field in step 3 is used, and no entry is required here.
- o For **IKE with X.509 Certificates (Main Mode and Aggressive Mode)**, enter the Peer ID you want to use in the appropriate field, either **Peer Distinguished Name**, **Peer Email Address** or **Peer Domain Name**, depending on the **Peer ID Type** specified for the IKE Proposal (VPN > IKE Proposal).



Note If you have selected aggressive mode and are using email or domain for the local ID, you must have configured the local email or domain name on the IPSec Configuration page.

- For **Manual Keying**:
 - o From the **Encryption** drop-down list, select the encryption method and enter the key. For details, see the [“Encryption” on page 192](#).
 - o From the **Authentication** drop-down list, select the authentication method and enter the key. For details, see [“Authentication” on page 192](#).
 - o In the **Incoming SPI (hex)** and **Outgoing SPI (hex)** fields respectively, enter unique hexadecimal values (from 1 to 8 characters) for the incoming and outgoing SPI. For details, see [“Incoming SPI \(hex\)” on page 192](#).

You must use the same key information on the remote device.

- STEP 10** For IPSec tunnel connections (site-to-site), configure the **Tunnel Setup** for the Local Network and Remote Networks:

STEP A In the **Tunnel Setup**, check **Enable IPSec Tunnel connections**.

STEP B In the **Local Networks** table, select the source IP addresses that the originating device allows to route VPN traffic to the peer VPN Firewall, for the specific security association. This applies only to IPSec tunnel mode connections.

- To use specific IP addresses for routing, select **IP Address group, IP Subnet, or IP Range**. Then, configure the value(s) for the selected field.
- If you have configured the remote (peer) device to use the tunnel as the default route (overriding the default gateway), select **Peer uses tunnel as default route**.
- To use DHCP Relay over VPN, select **Local addresses assigned by DHCP through this tunnel**.

STEP C In the Remote Networks table, select the destination IP addresses that the terminating X family or network device allows to route VPN traffic to the local VPN firewall, for the specific security association.

- To use specific IP Addresses for routing, select **IP Address, IP Subnet, or IP Range**. Then, configure the value(s) for the selected field.
- To override the default gateway, select **Use Tunnel as default route**. Only one SA may be configured with this option.
- To use DHCP Relay over VPN, select **Remote addresses assigned by DHCP through this tunnel**.

STEP 4 Click **Save/Create** to save the configuration.

Click **Cancel** to return to the IPSec Summary without saving the changes.

Edit the Default SA for Site-to-Site VPN Connections

STEP 1 From the LSM menu, select **VPN >IPSec Status**. Then, select the **IPSec Configuration** tab. The VPN - IP Security/ IKE page displays.

STEP 2 On the IPSec Configuration page in the **IP Security Associations** table, click the **Pencil** icon to for the **Default** SA entry.

STEP 3 On the Edit IP Security Association page, in the **IP Security Association Setup** table, check **Enable Security Association** to enable the Default SA.

STEP 4 For **IKE Setup**, select the **IKE Proposal** from the drop-down list of proposals currently configured.

STEP 5 If you have selected an IKE Proposal with pre-shared key (PSK), type the **Shared Secret**. If you have selected a proposal with X.509 Certificates, type the certificate key.

The same pre-shared key or X.509 Certificate and key must be available on any remote device using this IKE proposal to establish a VPN connection.

STEP 6 For **IPSec Tunnel Setup**, check **Enable IPSec Tunnel connections** if you want to use the Default SA as the tunnel mode for terminating the site-to-site connection:

All devices within the termination zone have unrestricted access to the VPN. Traffic received over the VPN has unrestricted access to all devices within the termination zone. Firewall rules must be configured to access other zones.

STEP 7 Click **Save** to save the configuration.

Click **Cancel** to return to the IPSec Configuration page without saving the changes.

IKE Proposal

Internet Key Exchange (IKE) is used to negotiate the keying material used by the IPSec VPN encryption and integrity algorithms. IKE uses UDP port number 500 and precedes the actual IPSec data flow. IKE is a two-stage mechanism for automatically establishing IPSec tunnels with dynamically generated keying material.

IKE Proposals are divided into two phases:

- The device negotiates **Phase 1** of the IKE and establishes a shared, secure connection. Phase 1 uses Aggressive Mode or Main Mode for packet exchange. The default is Main Mode.
- In **Phase 2**, the device establishes keying material for the VPN. Phase 2 is much quicker than Phase 1, since it can rely on the checks established during Phase 1, without needing to re-establish a shared, secure connection. Phase 2 uses Quick Mode for packet exchange.

Phase 1 of the IKE negotiation requires authentication between the two devices to be connected over the VPN tunnel. When you configure the IKE proposal, you can select one of the following Authentication methods based on your network security requirements.

- IKE with Pre-shared Key (Main Mode)
- IKE with Pre-shared Key (Aggressive Mode)
- IKE with X.509 Certificates (Main Mode)
- IKE with X.509 Certificates (Aggressive Mode)
- Manual Keying



Note To use the X.509 Certificate Authentication, you must first import matching X.509 CA Certificates and Local Certificates on the X family and the remote device (s). On the X family device, you can create certificates from the X.509 Certificates page (**Authentication > X.509 Certificates**).

On the X family device, you configure the IKE proposals with the authentication and encryption configuration (used for Phase 1 and Phase 2 IKE negotiation) required for the different types of remote devices that will connect via the VPN tunnel connection. Then, when you create the IPSec Security Association required for each remote device, you can select the IKE proposal to use for key exchange and specify the key information.

For additional information, see the following topics:

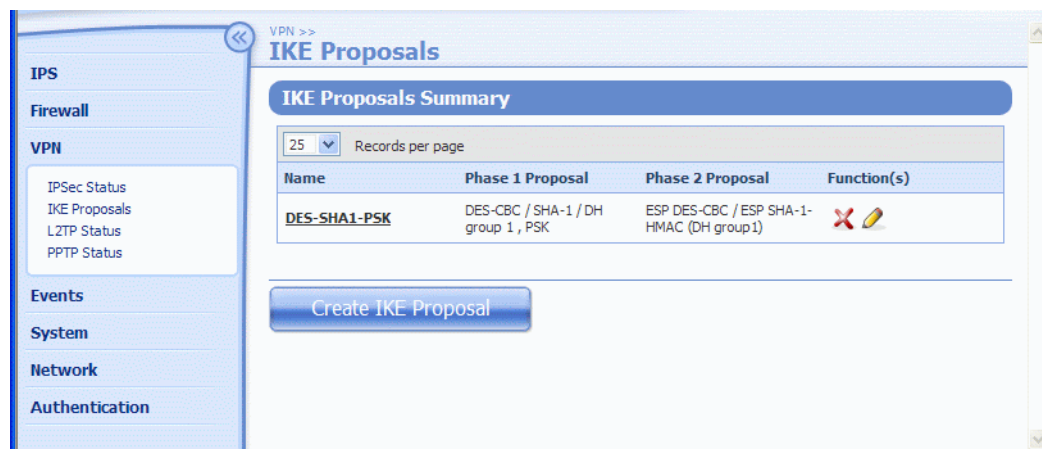
- [“Manage IKE Proposals” on page 198](#)
- [“Configuring IKE Proposals” on page 200](#)

Manage IKE Proposals

You can view, manage and configure IKE proposals from the IKE Proposals menu page (**VPN > IKE Proposals**) in the LSM.

The following figure shows the IKE Proposals summary page.

Figure 7–3: VPN: IKE Proposals Page



From this page you can complete the following tasks:

- View and manage existing IKE proposals configured on the device.
- Create/Edit an IKE Proposal
- Delete an IKE Proposal

For additional information, see the following topics:

- [“IKE Proposal Details” on page 199](#)
- [“Configuring IKE Proposals” on page 200](#)



IKE Proposal Details

The IKE Proposals page provides the following information about the existing proposals:

Table 7–4: VPN: IKE Proposal Details

Column	Description
Name	The name of the IKE Proposal
Phase 1 Proposal	The encryption and integrity protocols, the Diffie-Hellman (DH) Group number, and whether Aggressive Mode and NAT-Transversal (NAT-T) are enabled.
Phase 2 Proposal	The encryption and integrity protocols and the Diffie-Hellman (DH) Group number if using perfect forward secrecy

Table 7–4: VPN: IKE Proposal Details (Continued)

Column	Description
Functions  	Icons representing functions to manage IKE Proposals. The following functions are available: <ul style="list-style-type: none"> • Delete a proposal • Edit a proposal

Configuring IKE Proposals

IKE proposals provide the authentication and encryption methods that are used to configure the IPSec Security Associations for IPSec VPN tunnel. Configure an IKE proposal for each type of remote network device that requires a VPN connection.

Main Mode and Aggressive Mode

When you configure an IKE proposal, you have options to use main mode or aggressive mode. Main mode is the default and recommended configuration. You can use this mode if all the addresses of the remote sites to connect via VPN have fixed IP addresses. This is the recommended configuration. If the remote sites have dynamic addresses (not recommended), then you must use Aggressive mode for the IKE proposal. However, this mode is less secure.

You can configure an IKE Proposal from the Create/Edit IKE Proposal page (**VPN > IKE Proposal, create or edit**).

The following figure shows the Create/Edit IKE Proposal page:

Figure 7–4: VPN: Create/Edit IKE Proposal Page

Edit IKE Proposal

IKE Phase 1 Setup

Proposal Name: DES-SHA1-PSK

Encryption: DES-CBC

Integrity: SHA-1

Diffie-Hellman Group: 1 (768 bits)

Lifetime: 28800 seconds

Authentication Type: Pre-Shared Key

Options:

- ☐ Enable Aggressive Mode
- ☐ Enable NAT Traversal
- ☒ Enable Dead Peer Detection
- ☐ Automatically connect on system start-up
- ☒ Delete Phase 2 SA when Phase 1 SA terminates

IKE Phase 2 Setup

Encryption: ESP DES-CBC

Integrity: ESP SHA-1-HMAC

Lifetime: 3600 seconds

Diffie-Hellman Group: 1 (768 bits)

Options:

- ☐ Enable Perfect Forward Secrecy
- ☐ Enable strict ID checking of local network
- ☒ Use ID of 0.0.0.0/0 for local and remote networks

Save Cancel

For additional information, see the following topics:

- [“IKE Proposal Configuration Parameters: Phase 1 and 2” on page 202](#)
- [“Configure Phase 1 Setup Parameters for an IKE Proposal” on page 206](#)
- [“Configure Phase 2 Setup Parameters for an IKE Proposal” on page 207](#)

IKE Proposal Configuration Parameters: Phase 1 and 2

The following table describe the IKE Phase 1 and Phase 2 Configuration parameters. To review the parameter descriptions for each set, see the following links:

- [“IKE Phase 1 Setup:” on page 202](#)
- [“IKE Phase 2 Setup:” on page 205](#)

Table 7–5: IKE Proposal Phase 1 and Phase 2 Configuration Parameters

Parameter	Description
IKE Phase 1 Setup: Specify the parameters the X family device uses to negotiate Phase 1 of the IKE to establish a shared, secure connection. Phase 1 uses Aggressive Mode or Main Mode for packet exchange. The default is Main Mode.	
Proposal Name	Specifies a name for the IKE proposal. When you configure an IPSec Security Association, this name is used to select the IKE proposal to be used with the SA.
Encryption & Integrity	<p>Encryption and Integrity work in combination to provide the degree of security required. Recommended combinations for IKE Phase 1 and IKE Phase 2 are listed below in order from least secure to most secure.</p> <ul style="list-style-type: none"> • DES-CBC encryption with MD5 or SHA1 integrity (not recommended) <p>The following combinations are recommended combinations for IKE Phase 1:</p> <ul style="list-style-type: none"> • DES-CBC encryption with MD5 or SHA1 integrity • 3DES-CBC (strong encryption device only) with MD5 or SHA1 integrity • AES-CBC-128 (strong encryption device only) with SHA1 integrity • AES-CBC-192 (strong encryption device only) with SHA1 integrity • AES-CBC-256 (strong encryption device only) with SHA1 integrity <p>DES should only be used if it is supported on the remote device(s)</p> <p>Note The strong encryption options are only available if the device is configured with strong encryption. To enable strong encryption functionality (3DES, 128-AES, 192-AES, 256-AES), install the correct Strong Encryption Service Pack for your device available from the TMC Web site.</p>
Diffie Hellman Group	<p>Diffie-Hellman is the protocol used to establish shared security, in order to prevent unauthorized access to the key negotiation. The higher the Diffie-Hellman Group number, the more secure the connection. For interoperability or export restrictions, you may need to select a lower group number. Supported groups are:</p> <ul style="list-style-type: none"> • 1 (768 bits) - This setting is not recommended • 2 (1024 bits) • 5 (1536 bits) (High encryption device only)

Table 7–5: IKE Proposal Phase 1 and Phase 2 Configuration Parameters (Continued)

Parameter	Description
Lifetime	Specify the length of time the security association remains valid before new authentication and encryption keys must be exchanged (between 1 and 65535 seconds, default 28800). A lower value increases security, but may be inconvenient, since the connection is temporary disabled.
Authentication Type: Pre-Shared Key	If selected, the device uses a shared password to authenticate access to the VPN connection. If you select this option and use the Aggressive Mode option, you need to specify a Local ID Type and Peer ID Type.
Authentication Type: X.509 Certificates	If X.509 Certificates is selected as the Authentication Type, select the Local Certificate to be used for authentication from the drop-down list. To specify a CA certificate to validate access to the VPN, check Only accept peer certificates signed by . Then select the CA certificate from the drop-down list. If you do not specify a certificate, the device will use any of the imported CA certificates available on the device. Note Import certificates from the X.509 Certificates page (Authentication > X.509 Certificates) menu option to upload CA Certificates and Local Certificates for use on the device.

Table 7-5: IKE Proposal Phase 1 and Phase 2 Configuration Parameters (Continued)

Parameter	Description
Options: Enable Aggressive Mode	<p>To enable Aggressive mode, check Enable Aggressive Mode. Aggressive Mode is required when using dynamic WAN IP addresses. However, this mode is less secure. By default, the device uses Main Mode. If you select aggressive mode, configure the Local ID and Peer ID information that will be used to authenticate the Phase 1 of the IPsec connection.</p> <p>If Pre-Shared Key is selected for authentication:</p> <ul style="list-style-type: none"> From the Local ID Type drop-down list, select the type of information the device will use to negotiate Phase 1 of the IPsec connection: IP Address, Email Address, or Domain Name. <p>The values for the Local ID Email Address and Domain Name are configured on the IPsec Configuration page. The Local ID IP address value is the external IP address.</p> <ul style="list-style-type: none"> From the Peer ID Type drop-down list, select the type of information the device will use to negotiate Phase 1 of the IPsec connection: IP Address, Email Address, or Domain Name. <p>The values for the Peer ID IP Address, Email Address, and Domain Name are configured from the Create/Edit IP Security Association page.</p> <p>If X.509 Certificate is selected for authentication:</p> <ul style="list-style-type: none"> The Local ID Type defaults to Distinguished Name. From the Peer ID Type drop-down list, select the type of information in the X.509 certificate that the device will use to negotiate Phase 1 of the IPsec connection: Distinguished Name, Email Address, or Domain Name. Enter the appropriate information that is contained in the certificates on the device and on the remote device.
Enable NAT Traversal	Select this option if there is a NAT device between the two VPN devices.
Enable Dead Peer Detection	Check this option to enable the device to check that the VPN link is still functioning.
Automatically connect phase 1 on system start-up	Check this option to initiate the VPN upon startup with IKE phase 1 proposal automatically established. Use this option if the device is using a dynamic WAN IP address.
Automatically connect phase 2	This option is enabled if “Automatically connect phase 1 on system start-up” is checked.

Table 7-5: IKE Proposal Phase 1 and Phase 2 Configuration Parameters (Continued)

Parameter	Description
Delete Phase 2 SA when Phase 1 SA terminates	<p>Check this option to delete all Phase 2 security associations if the Phase 1 security association terminates.</p> <p>If this is selected, it can improve interoperability with VPN devices that automatically delete all the Phase 2 security associations if the Phase 1 security association terminates.</p>
<p>IKE Phase 2 Setup: Specify the parameters the device uses to negotiate phase 2 of the IKE to establishes keying material for the VPN. Phase 2 is much quicker than Phase 1, since it can rely on the checks established during Phase 1, without needing to reestablish a shared, secure connection. Phase 2 uses Quick Mode for packet exchange.</p> <p>Note If “Automatically connect phase 1 on system start-up” and “automatically connect phase 2” are both checked in IKE Phase 1 Setup, then after a phase 1 connection is established, every defined phase 2 connection is negotiated with the peer and brought up. Traffic can flow through the tunnel without further negotiation.</p>	
Encryption & Integrity	Encryption and Integrity work in combination to provide the degree of security required. For a list of combinations for IKE Phase 1 and IKE Phase 2, see “Encryption & Integrity” on page 202 .
Lifetime	<p>The duration of IKE Phase 2 (between 1 and 65535 seconds, default 28800). IKE Phase 2 will time out after this interval expires.</p> <p>Note This feature must be supported by the device by both VPN devices.</p>
Enable Perfect Forward Secrecy	Check this option to enhance VPN security if the remote device also supports the Perfect Forward Secrecy feature.
Diffie-Hellman Group	<p>This setting is only required if Perfect Forward Secrecy is enabled.</p> <p>Diffie-Hellman is the protocol used to establish shared security, in order to prevent unauthorized access to the key negotiation. The higher the Diffie-Hellman Group number, the more secure the connection. For interoperability or export restrictions, you may need to select a lower group number. Supported groups are:</p> <ul style="list-style-type: none"> • 1 (768 bits) • 2 (1024 bits) • 5 (1536 bits) (High encryption device only)

Table 7–5: IKE Proposal Phase 1 and Phase 2 Configuration Parameters (Continued)

Parameter	Description
Phase 2 Local ID configuration options	<p>These options determine how the device negotiates IKE Phase 2 local-id checking:</p> <ul style="list-style-type: none"> • Select Enable strict ID checking of local network to restrict the use of the Phase 2 tunnel to packets with a source IP address corresponding to a local-id configured for the local network of the IPSec security association. For backwards compatibility with the 2.2 release, this field is disabled by default. • Select Use ID of 0.0.0.0/0 for local and remote networks to create a single phase 2 SA for all traffic using local ID of 0.0.0.0/0 and remote ID of 0.0.0.0/0. This option allows interoperability with devices from other vendors such as Netscreen which always negotiate Phase 2 IDs as 0.0.0.0/0.

Configure Phase 1 Setup Parameters for an IKE Proposal

The values specified for Phase 1 IKE negotiation must match the values configured on the remote device.

- STEP 1** From the LSM menu, select **VPN > IKE Proposals**. The VPN - IKE Proposals page displays.
- STEP 2** On the IKE Proposals page, click **Create**, or to edit an existing IKE proposal, click its **Pencil** icon.
- STEP 3** If you are creating a new proposal, type the **Proposal Name**.
You cannot change the name of an existing proposal.
- STEP 4** Select the required encryption and integrity combinations from the **Encryption** and **Integrity** drop-down lists.
For information on these fields, refer to [“IKE Proposal Configuration Parameters: Phase 1 and 2” on page 202](#).
- STEP 5** Select the **Diffie-Hellman Group** from the drop-down list.
- STEP 6** In the **Lifetime** field, enter the length of time you want the security association to last before new authentication and encryption keys must be exchanged (between 1 and 65535 seconds, default 28800).
A lower value increases security, but may be inconvenient, since the connection is temporary disabled.
- STEP 7** From the **Authentication Type** drop-down list, select the method to use for authenticating access to the VPN:
- **Pre-Shared Key** — default level of security
 - **X.509 Certificates** — highest level of security
- STEP 8** Optionally, check **Enable Aggressive Mode** if the external IP address is not fixed. This setting is not recommended.

STEP 9 If you are using **Pre-Shared Key** with **Aggressive Mode**:

- From the **Local ID Type** drop-down list, select the identifier for the device to use for validation purposes, either **IP Address**, **Email Address**, or **Domain Name**.
- From the **Peer ID Type** drop-down list, select the identifier for the device to use for validation purposes, either **IP Address**, **Email Address**, or **Domain Name**.

You must select the same Local ID and Peer ID types that are configured on the remote device that will connect via the VPN tunnel.

STEP 10 If you are using **X.509 Certificates** (with either **Aggressive Mode** or **Main Mode**):

- Select the Local Certificate you want to use from the **Local Certificate** drop-down list
- Select the type of information in the certificate to use for validation purposes from the **Peer ID Type** drop-down list, either **Distinguished Name**, **Email Address** or **Domain Name**. You must select the same type that is used on the remote device.
- To specify the CA certificate you want to use to validate access to the VPN, check **Only accept peer certificates signed by**, and select the certificate from the drop-down list. This increases security on the VPN



Note If you do not specify a certificate, the device will by default use any of the available CA certificates. CA Certificates are imported from the X.509 Certificates page (**Authentication > X.509 Certificates**).

STEP 11 If there is a NAT device between the two VPN devices, check **Enable NAT-Traversal**.

STEP 12 To enable the device to check that the VPN link is still functioning, check **Enable Dead Peer Detection**.

STEP 13 To initiate the VPN upon startup with IKE phase 1 proposal automatically established, check **Automatically connect phase 1 on system start-up**.

Use this option if the device is using a dynamic external IP address.

If this option is checked, and you want to configure phase 2 connections to connect automatically, check **Automatically connect phase 2**.

STEP 14 To delete all Phase 2 security associations if the Phase 1 security association terminates, check **Delete Phase 2 SA when Phase 1 SA terminates**.



Note Some VPN devices automatically delete all the phase 2 security associations if the phase 1 security association terminates. To improve interoperability with such devices, check this option.

Configure Phase 2 Setup Parameters for an IKE Proposal

STEP 1 Select the required encryption and integrity combinations from the **Encryption** and **Integrity** drop-down lists.

STEP 2 Enter the duration of IKE Phase 2 in the **Lifetime** field (between 1 and 65535 seconds, default 28800). IKE Phase 2 will time out after this interval.

- STEP 3** To provide enhanced security, check **Enable Perfect Forward Secrecy**, and then select the **Diffie-Hellman Group** to use from the drop-down list.



Note This feature must be supported by both VPN devices.

- STEP 4** Configure the Phase 2 Local ID checking options to determine how the X family device negotiates IKE Phase 2 local-id checking. For details, see [“Phase 2 Local ID configuration options” on page 206](#).

- STEP 5** Click **Create/Save** to save the configuration.

Click **Cancel** to return to the VPN - IKE Proposals page without saving the changes.

For detailed field descriptions, see [“IKE Proposal Phase 1 and Phase 2 Configuration Parameters” on page 202](#).

L2TP Configuration

Overview

Layer 2 Tunneling Protocol (L2TP) allows a dial-up user to make a virtual Point-to-Point Protocol (PPP) connection to an L2TP Server on the VPN. L2TP sends PPP frames through a tunnel between a user and the L2TP Server.

You can configure the X family device to act as an **L2TP Server** with support for L2TP over IPSec. **L2TP over IPSec** is a combination of protocols commonly used to authenticate a user (L2TP) and encrypt data (using IPSec). It is much more secure than L2TP protocol alone.

As an L2TP Server, the device can terminate L2TP connections from VPN clients, such as those included with Windows XP or Windows Vista.



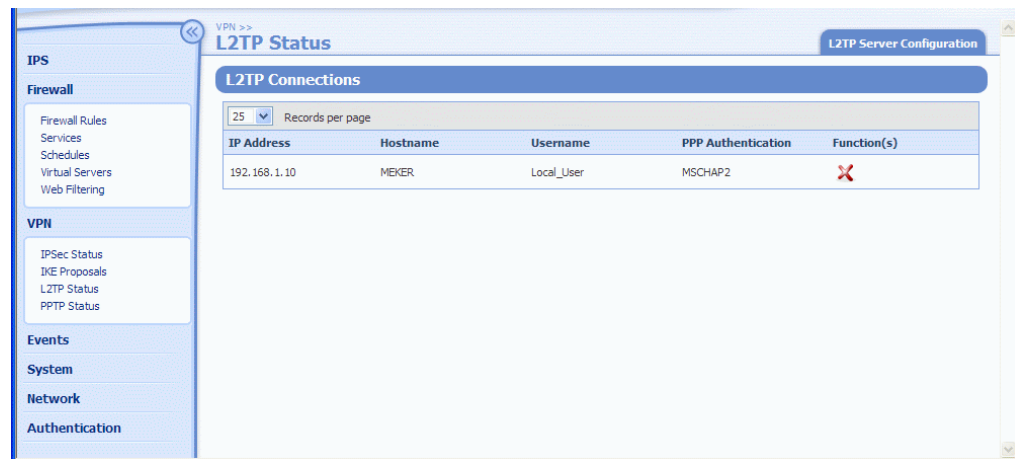
Note To use the device as an L2TP VPN terminator, you must check **Support L2TP** when you are configuring the IPSec default SA. For details, see [“Edit the Default SA for Client-to-Site VPN Connections using L2TP over IPSec” on page 194](#) for more information.

L2TP Status

You can view and manage L2TP connections and configuration from the L2TP Status page (**VPN > L2TP Status**).

The following figure shows the L2TP Status page:

Figure 7–5: VPN: L2TP Status Page




From this page, you can complete the following tasks:

- View current L2TP connections on the device
- Terminate a current connection
- Access the L2TP Server Configuration page to enable and configure the L2TP server for the X family device

L2TP Status Page Details

The **L2TP Connections** table provides the following information about current connections:

Table 7–6: VPN: L2TP Status Page Details

Column	Description
IP Address	The IP address allocated to the L2TP client
Remote IP Address	The public IP address of the L2TP client.
Hostname	The name of the device hosting the L2TP client
Username	The name used by the client for authentication by the local database or RADIUS
PPP Auth	The Point-to-Point Protocol (PPP) Authentication mechanism, either PAP , CHAP , MS CHAP or MS CHAPv2
Functions 	Icons representing functions to manage the L2TP connection: <ul style="list-style-type: none"> • Delete the current connection. Deleting a connection disconnects the remote user (client-to-site configurations) or network (site-to-site configurations) using the VPN link.

For additional information, see the following topics:

- [“L2TP Server Configuration” on page 210](#)
- [“Enable L2TP Server and Configure L2TP Client and Addresses” on page 211](#)

L2TP Server Configuration

You can configure the X family device to act as an L2TP server from the L2TP Server Configuration page (VPN > L2TP Status, L2TP Server Configuration tab).

The following figure shows the L2TP Server Configuration page:

Figure 7–6: VPN: L2TP Server Configuration Page

L2TP Server Configuration Parameters

The following table provides descriptions for the L2TP Server Configuration Parameters:

Table 7–7: L2TP Server Configuration Parameters

Parameter	Description
L2TP Server	
Enable L2TP Server	If checked allows VPN clients to use the X family device a VPN terminator for L2TP
L2TP Security Zone	Select the remote security zone on which to terminate the VPN from the L2TP Security Zone drop-down list.
Require Encryption	If checked, enables Microsoft Point-to-Point Encryption to provide additional security. This feature is supported by Windows VPN clients.
L2TP Client Configuration	

Table 7–7: L2TP Server Configuration Parameters

Parameter	Description
WINS Servers	If you are using Microsoft Networking, type the IP addresses of your primary (WINS Server 1) and secondary (WINS Server 2) WINS servers.
DNS Servers	Determines the DNS servers that the PPTP Server uses: <ul style="list-style-type: none"> • Select Device Acts as DNS Relay to enable the X family device to act a proxy-DNS server (DNS relay), passing DNS queries to its configured DNS servers. • Select Specify DNS Server to enter up to two local DNS server IP addresses, in order in which they are to be accessed, in the DNS Server fields.
L2TP Addresses	Determines how IP addresses are allocated to clients connected through the L2TP server: <ul style="list-style-type: none"> • Select IP address assigned by RADIUS to enable the X family device to use the RADIUS server to assign the L2TP client IP address. The RADIUS server must be enabled on the RADIUS page (Authentication > RADIUS). • Specify IP Address Group and select an existing address group to enable the X family device to assign the L2TP client an IP address from the addresses included in the IP Address group. Use the IP Addresses page (Network > Configuration > IP Address Groups) to create IP Address Groups.

[L2TP Configuration](#)

[Enable L2TP Server and Configure L2TP Client and Addresses](#)

Enable L2TP Server and Configure L2TP Client and Addresses

- STEP 1** If you are not using RADIUS to assign IP addresses, create an IP address group (**Network > Configuration > IP Address Groups**) containing the pool of IP addresses that the X family device will use to allocate IP addresses to L2TP VPN clients.
- STEP 2** From the LSM menu, select **VPN > L2TP Status**. Then click the L2TP Server Configuration tab.
- STEP 3** On the L2TP Server Configuration page, check **Enable L2TP Server**.
This allows VPN clients to use the X family as a VPN terminator for L2TP.
- STEP 4** Select the remote security zone on which to terminate the VPN from the **L2TP security zone** drop-down list.
- STEP 5** To use Microsoft Point-to-Point Encryption, check **Require encryption**.
This option provides additional security, and is supported by Windows VPN clients.
- STEP 6** To use Microsoft Networking, enter the IP addresses of your primary and secondary WINS servers in the **WINS Server 1** and **WINS Server 2** fields respectively.

STEP 7 To configure your **DNS Servers**, either:

- Select **Device Acts as DNS Relay** if you want the X family to act as a proxy-DNS server (DNS relay), passing DNS queries to its configured DNS servers
- Select **Specify DNS Server** and enter up to two local DNS server IP addresses, in the order in which they are to be accessed, in the **DNS Server** fields

STEP 8 To assign L2TP IP Addresses, either:

- Select **IP Address Assigned by RADIUS**, if you want the X family to use the RADIUS server to assign the L2TP client IP address
- Select **IP Address Group** and select an existing group from the drop-down list, if you want the X family to use an IP address group for the client

STEP 9 Click **Apply** to save the changes.

PPTP Configuration

Overview

Point-to-Point Tunnelling Protocol (PPTP) is an encrypted VPN protocol like IPSec, although not as secure as IPSec. PPTP does not support gateway to gateway connections and is only suitable for connecting remote users. A PPTP Server can terminate PPTP connections from VPN clients, such as those included with Windows 2000.

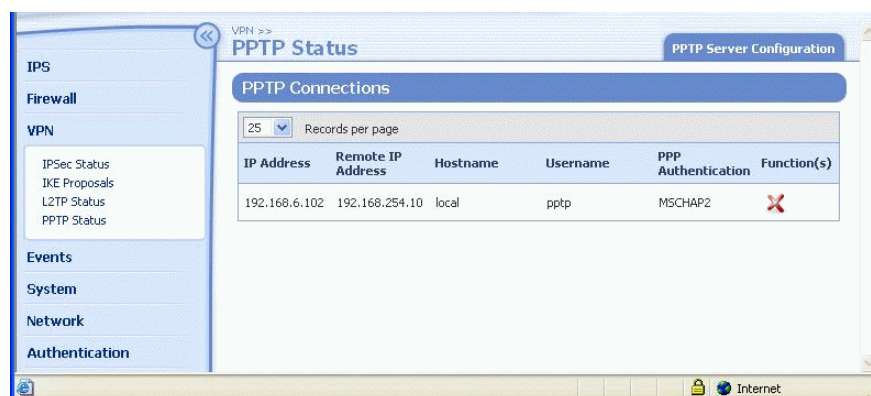
You can configure the X family to act as a **PPTP Server** for VPN termination that is compatible with Windows PPTP VPN clients such as Windows 98 and Windows 2000. The PPTP Server function also supports MPPE 128-bit encryption.

PPTP Status

You can view and manage PPTP connections and configuration from the PPTP Status page (**VPN > PPTP Status**).

The following figure shows the PPTP Status page:

Figure 7–7: VPN: PPTP Status Page




From this page, you can complete the following tasks:

- View current PPTP connections on the device
- Terminate a current connection
- Access the PPTP Server Configuration page to enable and configure the PPTP server for the X family device.

PPTP Status Page Details

The **PPTP Connections** table provides the following information about current connections:

Table 7–8: VPN: PPTP Status Page Details

Column	Description
IP Address	the IP address allocated to the PPTP client
Remote IP Address	The public IP address of the PPTP client.
Hostname	the name of the device hosting the PPTP client
Username	the name used by the client for authentication by the local database or RADIUS
PPP Authentication	the Point-to-Point Protocol (PPP) Authentication mechanism, either PAP , CHAP , MS CHAP or MS CHAPv2
Functions 	Icons representing functions to manage the PPTP connection: <ul style="list-style-type: none"> • Delete the current connection. Deleting a connection disconnects the remote user using the VPN link.

For additional information, see the following topics:

- [“PPTP Server Configuration” on page 213](#)
- [“Enable PPTP Server and Configure PPTP Client and Addresses” on page 215](#)

PPTP Server Configuration

You can configure the X family device to act as an PPTP server from the PPTP Server Configuration page (VPN > PPTP Status, **PPTP Server Configuration** tab).

The following figure shows the PPTP Server Configuration page:

Figure 7–8: VPN: PPTP Server Configuration Page

The screenshot shows the 'PPTP Server Configuration' page. On the left is a navigation menu with links for IPS, Firewall, VPN, Events, System, Network, and Authentication. The 'VPN' section is expanded, showing sub-links for IPsec Status, IKE Proposals, L2TP Status, and PPTP Status. The main content area is titled 'PPTP Server Configuration' and contains three main sections: 'PPTP Server', 'PPTP Client Configuration', and 'PPTP Addresses'. In the 'PPTP Server' section, 'Enable PPTP Server' is checked, 'PPTP Security Zone' is set to 'LAN', and 'Require Encryption' is checked. The 'PPTP Client Configuration' section has 'WINS Servers' and 'DNS Servers' fields. The 'PPTP Addresses' section has 'Specify IP Address Group' selected with 'VPN_Pool' as the value. An 'Apply' button is at the bottom.

PPTP Server Configuration Parameters

The following table provides descriptions for the PPTP Server Configuration Parameters:

Table 7–9: VPN: PPTP Server Configuration Parameters

Parameter	Description
PPTP Server	
Enable PPTP Server	If checked, allows VPN clients to use the device as a VPN terminator for PPTP.
PPTP Security Zone	Select the remote security zone on which to terminate the VPN from the PPTP Security Zone drop-down list.
Require Encryption	If checked, enables Microsoft Point-to-Point Encryption to provide additional security. This feature is supported by Windows VPN clients.
PPTP Client Configuration	
WINS Servers	If you are using Microsoft Networking, type the IP addresses of your primary (WINS Server 1) and secondary (WINS Server 2) WINS servers.
DNS Servers	Determines the DNS servers that the PPTP Server uses: <ul style="list-style-type: none"> Select Device Acts as DNS Relay to enable the device to act a proxy-DNS server (DNS relay), passing DNS queries to its configured DNS servers. Select Specify DNS Server to enter up to two local DNS server IP addresses, in order in which they are to be accessed, in the DNS Server fields.

Table 7–9: VPN: PPTP Server Configuration Parameters (Continued)

Parameter	Description
PPTP Addresses	<p>Determines how IP addresses are allocated to clients connected through the PPTP server:</p> <ul style="list-style-type: none"> • Select IP address assigned by RADIUS to enable the device to use the RADIUS server to assign the PPTP client IP address. The RADIUS server must be enabled on the RADIUS page (Authentication > RADIUS). • Specify IP Address Group and select an existing address group to enable the device to assign the PPTP client an IP address from the addresses included in the IP Address group. Use the IP Addresses page (Network > Configuration > IP Address Groups) to create IP Address Groups.



Note If PPTP Server is disabled, the table is not displayed and the message **PPTP Server is currently disabled** is displayed.

Enable PPTP Server and Configure PPTP Client and Addresses

- STEP 1** If you are not using RADIUS to assign IP addresses, create an IP address group (**Network > Configuration > IP Address Groups**) containing the pool of IP addresses that the X family device will use to allocate IP addresses to L2TP VPN clients.
- STEP 2** Select **VPN > PPTP Status**. Then click the **PPTP Server Configuration** tab.
- STEP 3** On the PPTP Server Configuration page, check **Enable PPTP Server**.
This allows VPN clients to use the device as a VPN terminator for PPTP.
- STEP 4** Select the remote security zone on which to terminate the VPN from the **PPTP security zone** drop-down lists.
- STEP 5** If you want to use Microsoft Point-to-Point Encryption, check **Require encryption**.
This provides additional security, and is supported by Windows VPN clients.
- STEP 6** If you are using Microsoft Networking, enter the IP addresses of your primary and secondary WINS servers in the **WINS Server 1** and **WINS Server 2** fields respectively.
- STEP 7** To configure your **DNS Servers**, either:
- Select **Device Acts as DNS Relay** if you want the device to act as a proxy-DNS server (DNS relay), passing DNS queries to its configured DNS servers
 - Select **Specify DNS Server** and enter up to two local DNS server IP addresses, in the order in which they are to be accessed, in the **DNS Server** fields
- STEP 8** To assign PPTP IP Addresses, either:
- Select **IP Address Assigned by RADIUS**, if you want the device to use the RADIUS server to assign the PPTP client IP address.
 - Select **IP Address Group** and select an existing group from the drop-down list, if you want the device to use an IP address group for the client.
- STEP 9** Click **Apply** to save the changes.

8 System

The System menu provides options to update and manage TOS and Digital Vaccine packages, configure timekeeping options, access for remote management applications (SMS & NMS), enable high availability to provide system failover, configure email and syslog servers, and access the setup wizard to change device and network configuration settings for the X family device.

Overview

The System menu in the LSM allows you to manage TOS and Digital Vaccine packages, change device configuration options, and configure access to external resources such as syslog and email servers and remote management applications. The System menu provides the following options:

- **Update** — View current software versions, update software, configure automatic Digital Vaccine (DV) updates, and manage system snapshots
- **Time Options** — Specify the timekeeping mechanism (internal clock or NTP) and time zone for the X family device.
- **SMS/NMS** — Enable remote management of the X family device.
- **High Availability** — Configure the X family device for high availability to provide a failover mechanism to minimize network downtime due to device failure.
- **Thresholds** — Specify the disk and memory usage settings that trigger major and critical usage level alarms on the Health Monitor and System Summary pages.
- **Email Server** — Configure the email server for the X family device to send event notifications.
- **Syslog Servers** — Configure remote syslog servers to maintain and backup data from the System, Audit, VPN, and Firewall Session logs.
- **Setup Wizard** — Configure critical device configuration settings to quickly install a new X family device on the network with internet access. The setup wizard can be reused to change system-wide configuration settings after the initial configuration is complete.

For details, see the following sections:

- [“Update TOS and Digital Vaccine Software” on page 218](#)
- [“Time Options” on page 229](#)
- [“SMS/NMS” on page 232](#)
- [“High Availability” on page 235](#)
- [“Thresholds to Monitor Memory and Disk Usage” on page 239](#)
- [“Email Server” on page 241](#)
- [“Syslog Servers” on page 242](#)
- [“Setup Wizard” on page 242](#)

Update TOS and Digital Vaccine Software

For up-to-date network protection, TippingPoint provides the following update options:

- TOS update package for the IPS device firmware and software
- Digital Vaccine Filter update package for IPS filters to provide protection for new and emerging network security threats

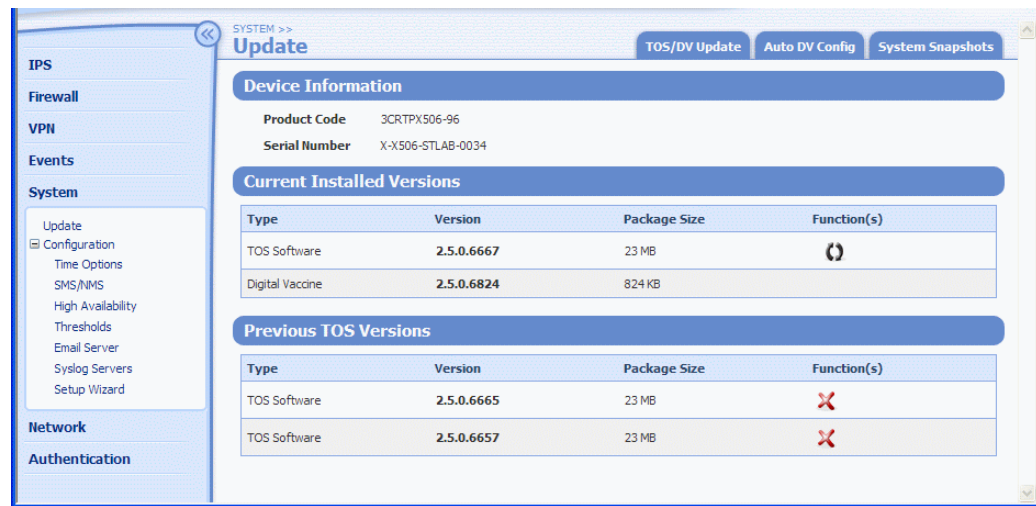
You can download software updates from the Threat Management Center (TMC) Web site (<https://tmc.tippingpoint.com>). Register for a TMC account from [eSupport.3com.com](https://esupport.3com.com). To create an account, you need the serial number of one of your X family devices and your customer ID. If you don't have the customer ID, contact your customer representative.

In the LSM, you can manage system software and digital vaccine filter packages from the Update page available on the System menu. From this page, you can:

- View current device information, installed TOS and Digital Vaccine version information, and a list of previously installed software
- Delete previous TOS versions to free disk space
- Perform a software rollback
- Download and install a TOS or DV Update
- Configure the Auto DV update function
- Create and manage System Snapshots

The following figure shows the Update page.

Figure 8–1: System: Update Page



For additional information, see the following topics:

- [“Viewing and Managing Current TOS and DV Software” on page 219](#)
- [“Delete a previously installed TOS software version” on page 221](#)
- [“Rolling Back to a Previous TOS Version” on page 220](#)
- [“Download and Install a TOS or Digital Vaccine Update” on page 221](#)
- [“System Snapshots” on page 227](#)



Viewing and Managing Current TOS and DV Software

The Update page provides information on the software for the X family device. From this page, you can:

- View information on the device model and on current and previously installed software versions
- Perform a software roll back
- Access the TOS/DV Update, Auto DV Config, and System Snapshot functions

The Update page provides the following information about the device and its software state.

Field	Description
Device Information:	
Product Code	The manufacturing code assigned to the X family device.
Serial Number	The serial number of the device. This number can be used to create an account to access the TMC Web site. You may also need this number when you contact Technical Support.

Field	Description
Current Installed Version:	
Type, Version Package Size	Identifies the properties of the current TOS software and Digital Vaccine versions installed on the device. Any functions available are listed in the function(s) column
Function(s): 	Any functions available are listed in the function(s) column. The rollback icon indicates that there is at least one prior version of the X family software on the device that you can rollback to. For details, see “Rolling Back to a Previous TOS Version” on page 220 .
Previous TOS Versions:	
Type, Version Package Size	Identifies the properties of previous TOS software packages that have been installed on the device. You can delete TOS software and Digital Vaccine versions installed on the device. Any functions available are listed in the function(s) column
Function(s): 	Any functions available are listed in the function(s) column. If you delete all previously installed TOS software versions, you cannot perform a software rollback.

Rolling Back to a Previous TOS Version



CAUTION To make sure you understand the effects of a software rollback, read the release notes for the current software version and the software version you are rolling back to before performing the rollback operation.

A rollback operation reverts the currently running software version on your X family device to a previous working version. The device retains settings and configurations. However, not all functionality may be available depending on the version of the TOS you roll back to. For details, refer to the release notes for that version of the software.

When you perform a rollback of the software, the Update page displays a set of status messages. See [“System Update Status Messages” on page 303](#) for details.

Persistent Settings

When you perform an operating system rollback, your current configuration settings are preserved, but filter settings roll back to the settings that were in effect when the rollback version was archived. Any changes to filter setting made after your target rollback version are deactivated, including attack protection filter updates.

Perform a Software Rollback



CAUTION If you perform a rollback, read the release notes for both the software version you are rolling back from and the software version you are rolling back to.



Note When you update and rollback, the LSM does not lose your settings or configurations.

STEP 1 On the Update page in the **Current Installed Versions** table, click the **Rollback** icon in the **Functions** column for the TOS Software.

A confirmation message displays.

The X family device deletes the current operating system files and reinstalls the previous operating system files. When the installation completes, the device performs a soft reboot.

STEP 2 After the device installs the previous TOS version, log back into the LSM.

To restore the operating system you rolled back from, you will need to reload it on your X family device. For more information, see the following topics:


- [“Software Update Process Overview” on page 225](#)
- [“Install a Software Update” on page 225](#)

Delete a previously installed TOS software version



CAUTION Unless the device is out of disk space, do not delete the previous TOS image that you were running. If the current TOS image becomes corrupted, you can roll back to the previous version as explained in [“Perform a Software Rollback” on page 221](#).

STEP 1 On the Update page in the **Previous TOS Versions** table, review the list of previous versions and decide which is safe to delete. Typically, there may be several versions. It is safest to delete the older files. You may want to keep the most recent version in case you need to perform a software rollback.

STEP 2 Click the  icon in the **Functions** column for the TOS software package you would like to delete. A confirmation message displays.

STEP 3 Click **OK**.

Download and Install a TOS or Digital Vaccine Update

You can download and install TOS and DV updates from the TOS/DV Update page.

When downloading and installing a software or Digital Vaccine package, verify that the package you download is not larger than the listed amount of free space. An unpacked package may require more space than anticipated, depending on your device model, saved snapshots and rollback versions, and the size of the available update. To make sure the device has enough disk space, you can delete previously installed software images from the Update page.

For additional information, see the following:

- [“Updating the Digital Vaccine \(Filters\)” on page 222](#)
- [“Updating the TOS Software” on page 224](#)

Updating the Digital Vaccine (Filters)

When new types of network attack are discovered, or when detection methods for existing threats improve, the Digital Vaccine team at the Threat Management Center (TMC) creates and releases new filters to add to your filter database. These filters are released as Digital Vaccine (DV) packages.

When a new DV package is available for download, the TMC team sends notifications to existing customers. You have two options to update the DV on your device:

- Configure the Auto DV option on your device so that the device can check for new DV packages and automatically update the device as necessary.

If AutoDV is configured, the device automatically checks the DV version when you open the Auto DV Configuration page. The status is listed in the **Auto Update** section. To perform an update immediately, click **Update Now**.

- Manually download and install the DV package.

You can manually download the most current DV from the Threat Management Center, and then manually install the DV update.



Note You cannot rollback to a previous Digital Vaccine version. If you want to use a previous version of a Digital Vaccine, select an older version of the Digital Vaccine package from the TMC.

To make sure the device has enough disk space, you may need to delete previously installed software images from the Update page. For details, see [“Delete a previously installed TOS software version” on page 221](#).

For additional information, see the following:

- [“Enable Auto Update for Digital Vaccine” on page 222](#)
- [“Manually Download a DV Update” on page 223](#)
- [“Manually Install a DV Update” on page 223](#)

Enable Auto Update for Digital Vaccine

- STEP 1** From the LSM menu, select **System > Update**. On the Update page, click the **Auto DV Config** tab.
- STEP 2** On the Auto DV Update page in the **AutoDV** table, click the **Enabled** check box to turn on the option.

When you select the check box, the scheduling fields appear so you can establish one of the following schedule types for the DV update process.

- **Periodic** — Performs an update every number of days starting from a set day. The option includes a time to perform the update.
- **Calendar** — Performs an update on a set day and time per week.

STEP 3 To set a **Periodic** update:

STEP A Enter the interval number of days.

STEP B Select a day of the week to begin the interval from.

STEP C Select the hour and minute for the update to be performed (military 24 hour time).

STEP 4 To set a **Calendar** update:

STEP A Select a day of the week to perform the update.

STEP B Select an hour and minute for the update to be performed (military 24 hour time).

STEP 5 Click **Apply**. To perform an update immediately, click **Update Now**.

Manually Download a DV Update

STEP 1 From the LSM menu, select **System > Update**. On the Update page, click the **TOS/DV Update** tab.

STEP 2 On the TOS & DV Update page in Step 1, click **Threat Management Center** to access the Threat Management Center.

STEP 3 Log in to the Threat Management Center. If necessary, create an account from the login page.

STEP 4 From the top menu bar on the TMC home page, select **Releases > Digital Vaccine** to display the list of digital vaccine filters available.

STEP 5 Click on the software update that you want to download. On the Software Details page, review the information about the package.



Note For DV packages, you cannot rollback to a previous version. To use a previous version, download that version from the TMC.

STEP 6 Click the **Download** tab to download the package to your local device. Make sure to note the download location and the file size.

Manually Install a DV Update

STEP 1 From the LSM menu, select **System > Update**. On the Update page, click the **TOS/DV Update** tab.

STEP 2 Verify available disk space.

STEP A In **Step 2** on the SYSTEM - Update - Manual Software Update page, locate the line that says:

Make sure the file you downloaded is smaller than: <number>

MB.

If the update package that you downloaded is smaller than <number>, proceed to Step 3.

- STEP B** If the update package is larger than <number>, delete older versions of the software to free disk space. For details see [“Delete a previously installed TOS software version” on page 221](#).

After freeing disk space, return to the TOS/DV Update page and repeat Step 2 and 3.

- STEP 3** In Step 3 check the **High Priority Enabled** check box if there is an immediate need for the update, and it is during normal working hours. This setting will give requests from the update process the highest system priority until the update completes.



Note The High Priority Enabled option provides the priority for downloading the package. However, the device does not give package installation processes priority over attacks. If an attack occurs during an update, the device will not give priority to the update process at that time.

- STEP 4** In Step 4, type the full path and file name for the update package that you downloaded from the Threat Management Center, or click **Browse** to select the file.

- STEP 5** Click **Install Package**.

While the new file is loaded onto your device, an Update Progress page displays the current status of the update. After the installation completes, you are returned to the Update page. The new version displays in the **Version** column of the **Current Installed Versions** table.

Updating the TOS Software

When improvements or additions are made to the X family device, we release a software update on the TMC Web site (<https://tmc.tippingpoint.com>). You can download and install updates from this site.



CAUTION You must read the release notes posted with the TOS software update package on the TMC. The release notes contain information that may make the difference between a successful software update and an unsuccessful software update.

When you perform an update of the software, the Update page displays a set of status messages. See [“System Update Status Messages” on page 303](#) for details.

Persistent Settings

When you perform a software update, your current configuration and filter settings are persisted forward.



Note When you install a software update, an archive copy of your current filters settings will be saved. If you perform a software rollback in the future, any changes made to your filters settings after the update will not be preserved.

During a graceful shutdown, as during an update or reboot (in the LSM or command in the CLI), Packet Trace data may not be automatically flushed to disk. To guarantee Packet Trace data is flushed to disk, do the following:

- Click on any Packet Trace icon in the alert or block logs
- Click on the Packet Trace (TCPDUMP) icon

Software Update Process Overview

The update procedure takes approximately 30 minutes for the entire procedure, depending on your download speed. The following table provides a summary of the process with time estimates.

Step	Task	Manual or Automatic	Estimated Time	Link Status
1	Download the package	Manual	Varies	Up
2	Install the package	Manual	15-20 minutes	Up
3	Reboot the device	Automatic	5 minutes	Down
4	Commit and update the changes	Automatic	A few seconds	Down

Download a TOS Software Update

STEP 1 Log into the LSM.

STEP 2 From the LSM menu, select **System > Update**. On the Update page, click the **TOS/DV Update** tab.

STEP 3 On the TOS & DV Update page in Step 1, click **Threat Management Center** to access the Threat Management Center.

STEP 4 Login to the Threat Management Center. If necessary, create an account from the login page.

STEP 5 From the top menu bar on the TMC home page, select **Releases > Software > modeltype > modelnumber**.

The model number and type is available on the LSM home page.

STEP 6 Click on the software update that you want to download. On the Software Details page, review the information about the package.

STEP 7 Click the **Download** tab to download the package to your local device. Make sure to note the download location and the file size.

After you have downloaded the update, you can install it from the LSM Update page. For details, see [“Install a Software Update” on page 225](#)

Install a Software Update

Prior to installing the new software, backup any custom filters you have created and implemented. The update will overwrite these files.

- STEP 1** If necessary, download a software update package from TMC.
- STEP 2** From the LSM menu, select **System > Update**. On the Update page, click the **TOS/DV Update** tab.
- STEP 3** Verify available disk space.
- STEP A** In Step 2 on the SYSTEM - Update - Manual Software Update page, locate the line that says:
 Make sure the file you downloaded is smaller than: <number> MB.
 If the update package that you downloaded is smaller than <number>, proceed to Step 3.
- STEP B** If the update package is larger than <number>, delete older versions of the software to free disk space. For details, see [“Delete a previously installed TOS software version” on page 221](#).
 After freeing disk space, return to the TOS/DV Update page and repeat Step 2 and 3.
- STEP 4** In Step 3 check the **High Priority Enabled** check box if there is an immediate need for the update, and it is during normal working hours. This setting will give requests from the software update process the highest system priority until the update completes.



Note The High Priority Enabled option provides the priority for downloading the package. However, the device does not give package installation processes priority over attacks. If an attack occurs during an update, the device will not give priority to the update process at that time.

- STEP 5** In Step 4, type the full path and file name for the update package that you downloaded from the Threat Management Center, or click **Browse** to select the file.
- STEP 6** Click **Install** to install the software update.

When updating the software, the bar showing update progress may be interrupted by a pop-up message window. If this occurs, you will need to monitor the update process using the system log. If the system log does not show any errors during the update process, the device reboots when the update is complete.

When the installation completes, the device performs a soft reboot. After the reboot, you can log back in to the device.



CAUTION During the LSM install, do not close the browser window or navigate off the Update page while the software installs.

System Snapshots

From the System Snapshots page, you can create, manage, restore and import local snapshots for the X family device. After restoring a snapshot, the device will always restart



CAUTION You can apply a single snapshot to multiple devices. However, applying the snapshot to devices managed by an SMS can cause a device ID conflict. Do not apply a snapshot to multiple devices when managed by SMS.

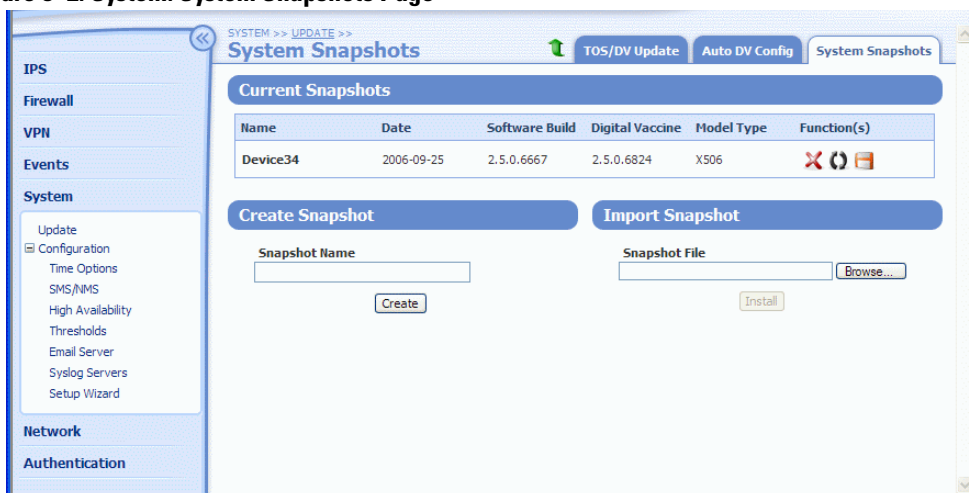
Do not perform an Update of your software while running a snapshot. The device may experience conflicts.

From this page, you can complete the following tasks:

- [“Create a Snapshot” on page 228](#)
- [“Import a Snapshot” on page 229](#)
- [“Restore a Snapshot” on page 229](#)
- [“Export a Snapshot” on page 229](#)
- [“Delete a Snapshot” on page 229](#)

The following figure shows the System Snapshots page:

Figure 8–2: System: System Snapshots Page



The System Snapshots page provides the following information:

Column	Definition
Name	Name of the snapshot
Date	The date the snapshot was generated
Software Build	The build number for the TOS software running when the snapshot was generated
Digital Vaccine	The version number of the Digital Vaccine package running when the snapshot was generated
Model Type	The model name of the device on which the snapshot was generated.
Functions	Icons representing functions to manage snapshots. The following functions are available: <ul style="list-style-type: none"> • Delete a snapshot • Restore A Snapshot • Import a snapshot


Create a Snapshot

- STEP 1** From the LSM menu, select **System > Update**. Then, click the option **System Snapshots** tab.
- STEP 2** On the System Snapshots page in the **Create snapshot** table, type a name for the snapshot.
- STEP 3** Click **Create**.

Import a Snapshot

- STEP 1** From the LSM menu, select **System > Update**. Then, click the **System Snapshots** tab.
- STEP 2** On the System Snapshots page in the **Import Snapshot** table, click **Browse** to select the file to import.
- STEP 3** Click **Install**. The selected snapshot uploads and displays in the list of snapshots.


Restore a Snapshot

- STEP 1** From the LSM menu, select **System > Update**. Then, click the **System Snapshots** tab.
- STEP 2** In the **Current Snapshots** table, locate the snapshot you want to restore.
- STEP 3** In the **Function(s)** column, click  (**Restore**). When you restore a snapshot, you replace all current settings with those from the snapshot. After restoring a snapshot, the device will always restart




CAUTION You can apply a single snapshot to multiple devices. However, applying the snapshot to devices managed by an SMS can cause a device ID conflict. Do not apply a snapshot to multiple devices when managed by SMS.

Export a Snapshot

- STEP 1** From the LSM menu, select **System > Update**. Then, click the **System Snapshots** tab.
- STEP 2** On the System Snapshots page in the **Current Snapshots** table, locate the snapshot you want to export.
- STEP 3** In the **Function(s)** column, click  (**Export**). When you export a snapshot, you save the snapshot to a local directory to later import if needed.

Delete a Snapshot

- STEP 1** On the launch bar, click the **Update** tab. The Update page displays.
- STEP 2** Select the **Open > System Snapshots** option. The Update - System Snapshots page displays.
- STEP 3** Locate the snapshot you want to delete. Click  (**Delete**).

Time Options

The X family device uses the system time in log files and also for schedule-based firewall rule configurations. To ensure Log file accuracy, facilitate log analysis, and establish predictable scheduling, configure the correct time zone and timekeeping mechanism before using the device in a live environment.

Use the Time Options page (**System > Configuration > Time Options**) to configure the timezone and timekeeping mechanism for the device:

- **Internal CMOS Clock** — Configures the device to keep time independently using its internal clock.
- **NTP Server** — Configures the device to synchronize its internal clock by querying user-defined Network Time Protocol (NTP) servers.
- **Time Zone** — Logs are kept in Universal Time (UTC or Greenwich Mean Time). Use this option to configure the time zone so that log times are translated into local values when displayed.

The following figure shows the Time Options page:

Figure 8–3: Time Options Page

SYSTEM >> CONFIGURATION >>
Time Options

Clock Source

☐ Internal CMOS clock

Set to Local Browser Time

CMOS Date: 2006-09-24 (YYYY-MM-DD)

CMOS Time: 02:54:48 (HH:MM:SS)

☒ NTP protocol

Duration: 5

Offset: 1

Fast Sync: 1

Server host: Port: Add to table below

Server	Port	Function(s)
10.100.230.118	123	✗
10.100.230.120	123	✗
10.100.230.143	123	✗
10.100.230.142	123	✗

Peer Host: Port: Add to table below

Peer	Port	Function(s)
------	------	-------------

Time Zone

GMT (Greenwich Mean Time), GMT 0:00 ☒ Automatically adjust clock for daylight saving changes

Apply

For additional information, see the following topics:

- [“Internal CMOS Clock” on page 231](#)
- [“NTP Server” on page 231](#)
- [“Time Zones” on page 232](#)

Internal CMOS Clock

Set the Internal CMOS Clock Time

- STEP 1** From the LSM, select **System > Configuration > Time Options**.
- STEP 2** On the Time Options page in the **Clock Source** table, click **Internal CMOS clock**.
- STEP 3** To automatically populate the date and time settings, click **Set Time to Local Browser Time**.
- OR**
- Type the **CMOS Date** and **Time** in the formats specified next to the fields.
- STEP 4** Click **Apply**.

NTP Server

To synchronize the system time on the X family device with an external time server (NTP server), select NTP as the clock source for your device. Using an NTP server, the device synchronizes time with the NTP server which allows the timing of network events on different hosts to be compared more accurately.



TIP To ensure that events times from different network entities can be meaningfully compared, configure the same NTP clients for the X family device and other network devices.



CAUTION Using external NTP servers could possibly make your device susceptible to a man-in-the-middle attack. It is more secure to use an NTP server on a local, protected network.

The following table provides information on the NTP protocol configuration parameters.

Parameter	Description
Duration	Interval at which the X family device will check with the time server. A zero value will cause time to be checked once on boot.
Offset	If the difference between the new time and the current time is equal to or greater than the offset, the new time is accepted by the device. A zero value will force time to change every time the device checks.
Fast Sync	If this field is set to 1, the X family device is allowed to trust the NTP server after the first time query. This sets the local time on the device immediately, but there is a risk that the set time will be incorrect. To disable this option, set this value to 0.
Server Host, Port	The IP address and Port for the NTP server
Peer Host, Port	

Configure the X family device for NTP Servers

- STEP 1** From the LSM menu, select **System > Configuration > Time Options**.
- STEP 2** On the Time Options page in the **Time Zone** table, click **NTP protocol**.
- STEP 3** Type the **Server host** IP address and **port** for the NTP server. Then, click **Add to table below**.
You can add multiple NTP server hosts.
- STEP 4** In the **Duration** field, type the interval at which the X family device will check the time server (in minutes).
A zero value will cause time to be checked once on boot.
- STEP 5** In the **Offset** field, type the allowable time difference between the server time and the current time.
If the difference between the new time and the current time is equal to or greater than the offset, the device accepts the new time. Type zero to force the time to change every time the device synchronizes with the server.
- STEP 6** In the **Fast Sync** field, type 1 to allow the device to trust the NTP server after the first time query and immediately update the time.
For more accurate time synchronization, type 0 to disable the Fast Sync option.
- STEP 7** For each symmetric NTP server peer, type the **Peer Host** and **Port**. Then, click **Add to table below**.
- STEP 8** Click **Apply**.

Time Zones

Use the Time Zone configuration option to specify the X family device time zone. The default time zone for the device is Universal Time (UTC or Greenwich Mean Time). If you change the default, the LSM logs will display time data based on the specified time zone.

Set the Time Zone for the Device

- STEP 1** From the LSM menu, select **System > Configuration > Time Options**.
- STEP 2** On the Time Options page in the **Time Zone** table, select the correct **Timezone** from the drop down list.
- STEP 3** Click the check box to **Automatically adjust clock for daylight saving changes**.
- STEP 4** Click **Apply**.

SMS/NMS

From a TippingPoint SMS, you can remotely monitor and manage X family devices. When an SMS is managing the device, you can view, manage, and edit the device configuration, and review logs and reports. You can also configure security zones and security policy (firewall rules, IPS filters, and traffic threshold filters) from the SMS and distribute the configuration to multiple X family devices.

From an NMS, you can remotely *monitor* the events and system status of the X family device. Configuring an NMS enables applications such as HP OpenView™ to monitor the device.

When a device is under SMS management, the message (DEVICE UNDER SMS CONTROL) displays in red at the top of each page in the LSM. In this state, you can view system configuration and status but editing is not available with the exception of Authentication configuration. The serial number and the IP address of the controlling SMS are displayed on the SMS and NMS page.

Configure and manage SMS and NMS systems from the SMS & NMS page in the LSM. From this page you can:

- [“Configure SMS Information” on page 234](#)
- [“View or Configure NMS Information” on page 235](#)
- [“Disable/Enable SMS Management” on page 235](#)

The following figure shows the Configure - SMS and NMS page:

Figure 8–4: Configure - SMS and NMS Page



CAUTION Communication between the X family device and the SMS or NMS is managed by the SNMP server which provides access to interface counters and other statistics, configuration data, and general system information via the Simple Network Management Protocol (SNMP). You enable the SNMP server by selecting the SNMP V2 option during the SMS/NMS configuration process. If you disable this option, SMS and NMS functionality is also disabled.

Additional Configuration Requirements

To communicate to the SMS, you may need to configure firewall rules on the X family device such that the following protocols are allowed between the device and the zone where the SMS resides:

- **HTTPS** (HyperText Transfer Protocol, Secure) — Protocol for handling secure transactions
- **SNMP** (Simple Management Network Protocol) — Protocol for managing nodes on an IP network and monitoring various types of equipment including computers, routers, and wiring hubs
- **NMS** (Network Management System) — Protocol for monitoring the device by a restricted NMS, such as HP OpenView

For more information about configuring the firewall, see [“Firewall” on page 63](#).

Configure SMS Information

STEP 1 From the LSM menu, select **System > Configuration > SMS/NMS**.

STEP 2 Type an **SMS Authorized IP Address/CIDR**.

The default value is *Any* which means that any SMS can manage the device. To specify a range of IP addresses, enter an IP address block (10.100.230.0/24, for example). This allows any SMS on the specified IP subnet to manage the device.

STEP 3 Verify that the **SNMP V2:Enabled** check box is selected.

STEP 4 Click **Apply**.



Note If the X family has previously been managed by an SMS, the serial number, IP address, and port for SMS displays.

View or Configure NMS Information

STEP 1 From the LSM menu, select **System > Configuration > SMS/NMS**.

STEP 2 On the SMS & NMS page in the Configure SMS table, verify that the **SNMP V2: Enabled** field is selected.

STEP 3 In the NMS Settings table, type **NMS Community String**. You can enter 1-31 characters for this string.

STEP 4 Type the **NMS Trap IP Address** and **NMS Trap Port**. Then, click Add to table below.
You can add multiple NMS Trap destinations. The X family device will send event and activity notifications to the specified destinations.

STEP 5 Click **Apply**.

Disable/Enable SMS Management

STEP 1 From the LSM menu, select **System > Configuration > SMS/NMS**.

STEP 2 If the device is currently being managed, remove the selection from the **SMS Control: Enabled** check box.

If the device is not currently under management and an SMS serial number and IP address display, click the **SMS Control: Enabled** check box to turn management control over to the the specified SMS.

If the device has never been managed by an SMS (the **Enabled** check box is not available), you can start managing it by logging into an SMS system with an authorized IP address. (for details on configuring an authorized IP address, see [“Configure SMS Information” on page 234](#).)

High Availability

X family devices support High Availability configuration to provide a failover mechanism to minimize network downtime due to device failure.

High availability requires two X family devices with the same configuration and licensing that are configured as a High Availability pair. One device is the active device. The second device is a standby device. The standby device constantly monitors the active device and automatically shifts from passive to active mode if the active device fails.

How High Availability Works

The following sections describe how high availability works in failover and standby mode and how the polling works to monitor the state of the active device. For details on configuring High Availability, see [“Configuration Overview” on page 237](#).

Failover Operation

After a pair of devices has been configured for high availability, the standby device only monitors the active device's HA state and does not route any network packets or monitor the dynamic behavior of the active device. If the standby device detects that the active device has failed, it will assume control of the IP interfaces used to route the packets on the network. When a device becomes active it sends an SNMP trap to any configured NMS trap destinations.

When a device takes over, it will not be aware of the final network state of the previous active device before it failed. This affects the device's network operation as follows:

- If dynamic routing is enabled, the new active device will start advertising its initial routing state and will need to relearn the network topology.
- TCP sessions that existed through the previously active device will be unknown to the new device and will be blocked. IPS and firewalling will only be performed on newly created sessions after the HA state transition.
- Site-to-site VPN tunnels that terminated on the previously active device will fail and will need to be re-established by the local device or its peer VPN terminator. To ensure that peer devices recognize a HA state transition and quickly re-establish tunnels, enable the Dead Peer Detection (DPD) option on IKE proposals.
- Client VPN connections (PPTP, L2TP and IPSec) will be closed and users will need to re-establish their VPN connection to the new active device using the same VPN IP address as before.
- The new active device will also be unaware of quarantined network equipment. However it will immediately establish quarantine for equipment that continues to transmit prohibited traffic.

When the device high availability state changes, the system generate messages in the system log. For a list of these messages, see [“High Availability Log Messages” on page 302](#).

Standby Operation

You can ping the HA management IP addresses from a network device such as a PC to check network connectivity to the standby device. However, the following network tools will not function properly from the console when a device is in Standby mode:

- Ping
- Traceroute
- Traffic Capture

As long as the device in Standby mode has the appropriate Digital Vaccine (DV) license, the device can automatically retrieve the latest DV updates to ensure the up-to-date protection when the device switches to Active mode. To enable this functionality, the DV website must be accessible directly from the external interface through a static route.

Polling

The High Availability function provides an optional polling feature that can be configured through the CLI. Polling is used to determine the regular heartbeat mechanism between the standby device and the active device. This function provides the following configuration parameters:

- **Poll-timer** determines the period in seconds that the standby device polls the active device. This, in turn, determines how quickly the standby device will detect that the active device has failed.

The active device should immediately respond to a poll from the standby device. If it does not, the standby device will retransmit the heartbeat message after a specified wait-interval in milliseconds.

A low poll timer increases the load on the network and can cause the standby device to become active due to lost poll requests or responses.

- **Retry-count** determines how many heartbeats the standby will send before it determines that the active device is not responding. If the active device does not respond to the heartbeats on any of the IP interfaces, the standby device will become the active device.

For details on configuring the high-availability polling feature, see the *Command Line Interface Reference*.

Configuration Overview

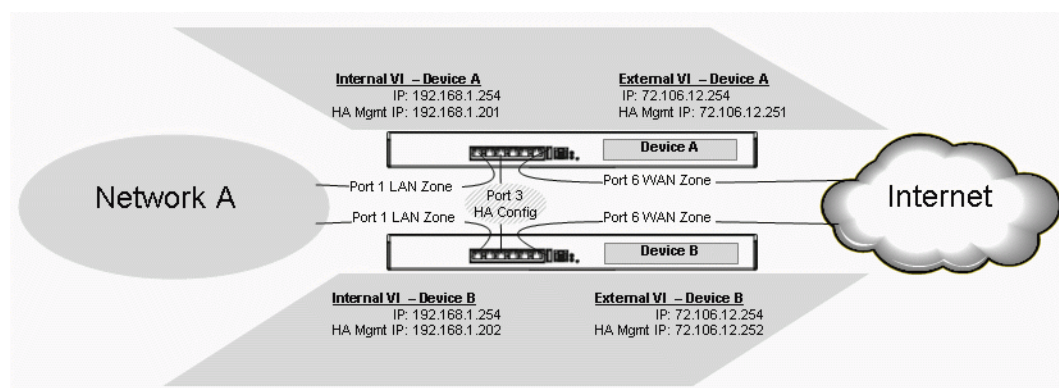
To use high availability, you need to configure a unique HA management IP address that can be used to manage the device from the network regardless of whether the device is in an active or passive state. In addition, we recommend that you configure a HA management IP address for each internal and external interface on the device. The IP addresses must conform to the following rules:

- The IP address for the external interface must be a static IP address.
- Each HA management IP addresses must be on the same IP subnet as it's respective IP interface.

When the devices are configured for High Availability, the devices use the HA management IP addresses to talk to each other and monitor the current state.

The following figure illustrates a simple HA deployment configured with a single IP interface and external IP interface.

Figure 8–5: High Availability Configuration



You can configure and manage High Availability from the High Availability page available from the LSM System menu. From this page you can:

- Configure an X family device for high availability
- Enable high availability
- Force a device to change its high availability state

Set up Devices for High Availability

STEP 1 Configure two X family devices with the same configuration.

STEP 2 Configure the network.

STEP A Connect the devices in parallel so that the respective ports on each device are connected together through a switch or similar device.

STEP B Shut down any unused ports and leave them disconnected.

STEP 3 Setup the zones and IP interfaces for the first device.

STEP A From the LSM menu, select **Network > Configuration > Security Zones**. Then, verify or create a LAN security zone on Port 1.

STEP B Select **Network > Configuration > IP Interfaces**. Then, create an internal interface for the LAN zone with NAT disabled. The IP address for this interface will be the same on both devices.

STEP C From the IP Interfaces page, create an external, static IP interface for the WAN zone. The IP address for this interface will be the same on both devices.

STEP 4 Configure and enable High Availability for the first device.

STEP A In the LSM menu, select **System > Configuration > High Availability**.

STEP B On the High Availability page in the **Communication Channel** table, specify a **HA Management IP Address** for the Internal and External interfaces.

STEP C To enable management of the device whether it is in Active or Standby mode, type a Management IP Address for the Internal MGMT interface.

You can use this address to access the device from the Management IP Address field.

STEP D Verify that the HA management IP address for each IP interface is on the same subnet as the IP interface. Then, make sure that the address specified for the external interface is a static IP address.

STEP E **Apply** the changes.

STEP 5 To set up the zones and IP interfaces for the second device, repeat Step 3.

When you configure the internal and external IP interfaces, use the same addresses that you entered for the first device.

STEP 6 Configure and enable High Availability for the second device.

STEP A On the High Availability page in the **Communication Channel** table, specify a HA Management IP Address for the Internal and External interfaces.

Enter IP addresses that are one host number higher than the addresses you entered for the first device. For example, if you entered 192.168.1.201 for the internal interface on the first device. Then, enter 192.168.1.202 for the second device.

STEP B **Apply** the changes.

Force High Availability State Change

If two devices are configured as a high-availability pair, one device is always Active mode while the other is in Standby mode. From the High Availability page, you can force a device to change modes.

STEP 1 Log into one of the devices in the High Availability pair.

STEP 2 From the LSM menu, select **System > High Availability**.

STEP 3 To change the current HA state of the device, click **Switch**.

It may take a moment for the device to change states.

Configuring High Availability with AutoDV

For the standby device to perform AutoDV, it needs a separate Digital Vaccine license.

The standby device uses the High Availability management IP address as the source IP address when doing AutoDV. Therefore, the HA management IP address must be public and routed to the Internet in addition to the external Virtual Interface IP address. When the active device does AutoDV it uses its external VI address.

If you have a separate (that is, the Internet side of the X family device) NAT device, then there is no need for a public IP address for either device so long as both can route to the Internet.

Troubleshooting High Availability with AutoDV

If the standby device cannot do AutoDV, check for the following:

- Verify that the primary device can do AutoDV. If so it suggests a routing or licensing issue.
- If the standby device cannot do AutoDV, can it do so if you make the standby device active? If so it suggests a licensing issue and not a networking issue.
- If the standby device cannot do AutoDV even when it becomes the primary device, and licenses have been checked, it suggests that the standby device has a problem routing to or from the Internet via its High Availability management IP address.

Thresholds to Monitor Memory and Disk Usage

From the LSM Health menu (**Events > Health > Monitor**), you can monitor current disk and memory usage levels for the X family device. The Monitor page has a State field that indicates whether usage is at normal, high, or critical levels. The settings that determine these levels are specified on the Thresholds page.

You can specify the following settings for the disk and memory thresholds:

- **Major Level** — Set the major threshold to a level that provides enough time to react before the situation is critical. For example, for disk usage, set a level where the disk is getting full, but is not so full that system activity is interrupted. The default value for both disk and memory usage is 90%.
- **Critical Level** — Set the critical threshold at a level that warns users *before* damage is about to occur. The default value for both disk and memory usage is 95%.

Set disk usage and memory thresholds

STEP 1 From the LSM menu, select **System > Thresholds**.

STEP 2 On the Thresholds page, specify the disk and memory thresholds.

STEP A For **Disk Usage Threshold**, enter a numeric value for the **Major Levels** and the **Critical Levels**. The major level value must be set lower than the critical level value.

STEP B For **Memory Usage Threshold**, enter a numeric value for the **Major Levels** and the **Critical Levels**. The major level value must be set lower than the critical level value.

STEP 3 Click **Save**.

To reset the values to the default settings, click **Reset to Defaults**.

For additional information, see [“Health” on page 116](#).



Note We recommend not modifying these values from their defaults.

Email Server

The X family device can be configured to send an email message when an IPS filter is triggered. The Email Server page allows you to configure the default email server settings to provide the email address, domain server, and SMTP address for the messages being sent from the device. After the email server settings have been configured, you can specify the email address contacts from the Notification Contacts page when you create or edit an action set.

The following figure shows the Email Server configuration page:

Figure 8–6: Email Server Page

Configure the Email Server

STEP 1 From the LSM menu, select **System > Configuration > Email Server**.

STEP 2 On the Email Server page, type the **Default To Email Address**.

This address displays in the **To Email Address** field when a user creates an email contact from the LSM.

STEP 3 Type the **From Email Address**.

This address is used as the **Reply-To** address for messages sent from the X family device.

STEP 4 Type the **From Domain Name**, such as `Acme . com`.

STEP 5 Enter the **SMTP Server IP Address**.

The device must be able to reach the SMTP server that will be handling the email notifications. You may have to add static routes (see [“Static Routes” on page 159](#)) so that the device can communicate with the SMTP server.

STEP 6 Enter a value for the **Email Threshold (per minute)**.

This limits the numbers of emails sent per minute.

STEP 7 Click **Apply**.

STEP 8 Click **Test Email** to verify your configuration settings.

For additional information on sending emails from the X family device, see [“Notification Contacts” on page 52](#).

Syslog Servers

To maintain and backup all log data from the X family device, you can configure remote syslog servers for system-related logs (System, Audit, VPN and Firewall Session logs).

For the Firewall Session Log, messages will only be off-loaded for firewall rules that have the *Enable syslog logging* option turned on.

The contents of the VPN Log can be customized to include messages to troubleshoot problems establishing a VPN tunnel.



Note You can also configure syslog servers for traffic-related event logging (entries in the Alert, IPS Block, and Firewall Block logs). For details, see [“Configure the Remote System Log Contact” on page 54](#).

Configure the Syslog Server Log Contact

STEP 1 From the LSM menu, select **System > Configuration > Syslog Servers**.

STEP 2 On the Syslog Servers page, select the **Enable syslog offload** option for each log you want to offload. Then, type the IP address for the remote server.



TIP Be sure that the device can reach the remote system log server on your network. If the server is on a different subnet than the device management port you may have to add static routes (see [“Static Routes” on page 159](#)).

For additional information, see the following topics:

- [“Logs” on page 98](#)
- [“Firewall Session Log” on page 103](#)
- [“VPN Log” on page 104](#)

Setup Wizard

The System Setup Wizard allows you to configure system settings from the LSM application. After you set up the X family hardware (see the *Quick Start Guide* for your device) and navigate to the default address for the LSM, the wizard automatically launches and steps through the configuration process. After the initial configuration, you can re-run the setup wizard if necessary by selecting **System > Configuration > Setup Wizard** from the LSM menu.

You can also setup the X family devices from an ssh command line using the CLI setup wizard. The CLI setup wizard provides additional options for configuring SMS and NMS management. The CLI Wizard is documented in the *Command Line Interface Reference*.

The following table lists the configuration steps included in the Setup Wizard along with links to documentation on the configuration task.

Table 8–1: Configuration Steps in Setup Wizard

Prompt	Description
Host Name & Location	Enter a name and physical location for the host. The name specified displays in the title bar of the browser window when a user is logged into the LSM application. The name is also used to identify the device when it is managed by an SMS or NMS.
Timekeeping Options	Specify the clock source (internal or NTP server) and time zone for the device. For details, see “Time Options” on page 229 .
IP Interfaces	Add or delete the IP interfaces that provide the X family with the interfaces to make the network connections required for your environment. An IP interface is the Layer 3 configuration for the device. For details, see “Static Routes” on page 159 .
Security Zones	Add or delete the security zones used to segment the network so that the X family device can apply security policy to traffic passing between the zones. For details, see “Security Zone Configuration” on page 135 .
Security Zone to IP Interface Mappings	Change the IP interface associated with each security zone. Each security zone must be associated with an internal or external IP interface so that it can be reached through the X family device. For details, see “Manage Security Zones for IP Interfaces” on page 149 .
DNS Settings	Configure DNS servers for the X family device. For details, see “DNS” on page 155 .
Web & CLI Management Options	Specify how the device can be managed through the LSM, through the CLI via SSH or both. You can also configure whether the web interface uses a secure (HTTPS) connection or an insecure HTTP connection.
Ethernet Port Configuration	Configure the line speed and duplex setting for the device’s Ethernet ports. For details, see “Network Port Configuration” on page 132 .
Email Configuration	Configure the email server so that the device can send event notifications. For details, see “Email Server” on page 241 .

9 Authentication

The Authentication section describes how to create and manage users accounts and configure the Privilege groups, RADIUS server and X.509 certificates used for VPN authentication.

Overview

The LSM Authentication menu pages enable Administrators to create and manage user accounts and configure authentication rules. The Authentication menu provides the following options:

- **User List** — create and manage user accounts to provide access to LSM operators and administrators and to provide local users with access to network services through the X family device.
- **Privilege Groups** — setup access rights for VPN clients and network services protected by firewall rules
- **RADIUS** — configure the X family device to use an external RADIUS server for user authentication
- **X.509 Certificates** — create, import and manage the CA Certificates, Certificate Requests, and Local Certificates used for VPN authentication
- **Preferences** — configure session and device timeouts, security level check required for passwords, and account login security

For additional information, see the following topics:

- [“User List” on page 246](#)
- [“Managing User Accounts” on page 249](#)
- [“How Local User Authentication Works: RADIUS, Privilege Groups and X.509 Certificates” on page 251](#)

User List

Overview

The User List menu pages allow you to create and manage user accounts to provide access to LSM operators and administrators and to provide local users with access to network services through the X family device. You can also configure authentication parameters that ensure secure access to the device and network services.

The following topics describe how user accounts and authentication are configured on the X family device:

- [“TOS and Local User Accounts” on page 247](#)
- [“TOS User Security Level” on page 247](#)
- [“Username and Password Requirements” on page 248](#)
- [“How Local User Authentication Works: RADIUS, Privilege Groups and X.509 Certificates” on page 251](#)

For instructions on using the User List menu options, see the following topics:

- [“Managing User Accounts” on page 249](#)
- [“Privilege Groups” on page 253](#)
- [“X.509 Certificates” on page 255](#)

TOS and Local User Accounts

The X family device has two types of user accounts:

A **TOS User** account provides access to the administrative interfaces of TOS to manage the device through the LSM web interface or from the Command Line Interface (CLI). The management functions available to a TOS user are determined by the account access level configured on the account. TOS users can only be defined in the embedded TOS user database on the device. TOS users cannot be configured in a RADIUS server.

The following levels are available:

- **Operator** — Base level administrator user who monitors device and network traffic
- **Administrator** — Enhanced administrator user who can view, manage, and configure functions and options in the device
- **Super-user** — Administrator user who has full access to the entire device

A **Local User** account provides controls on client access to network services through the device. Access to services is controlled through the X family device authentication mechanism. Local users cannot access the TOS administrative interfaces to manage the device. Local Users may be authenticated using the embedded user database within the TOS, or may be defined in a RADIUS server.

TOS User Security Level

For TOS user accounts, you can configure one of three access security levels:

- **Operator** — Base level administrator user who monitors device and network traffic
- **Administrator** — Enhanced administrator user who can view, manage, and configure functions and options in the device
- **Super-user** — Administrator user who has full access to the entire device



Note For local users, access to network services is controlled by Privilege Groups. For details, see [“Privilege Groups” on page 253](#).

The following table summarizes the functions available to users based on the Security Level access (Operator, Administrator, or Super-user) assigned to their user account.

Table 9–1: LSM Functions available to TOS Users based on Security Level

Functional Area	Operator	Administrator	Super-user
IPS/Quarantine	view	all	all
Firewall	view	all	all
Network	view	all	all
VPN	view	all	all

Table 9-1: LSM Functions available to TOS Users based on Security Level (Continued)

Functional Area	Operator	Administrator	Super-user
System	view	all	all
Events/Logs	view (except Audit log)	view all (except Audit log)	all
Update	view	all	all
Configure	view	all except system time	all
Admin	change own password view system log	change own password view system log	all, including change Idle Timeout change Password Expiration
Help	view	view	view

Username and Password Requirements

Restrictions on username and password values for user accounts are determined by the Security Level setting configured on the Preferences page. Username and password requirements are the same for local users and TOS users.

For the X family device, the default security access level is **Level 2, Maximum Security Checking**. For details on the available security levels and instructions for changing the security level, see [“Preferences Parameter Details” on page 267](#).

The following table provides examples of valid and invalid usernames and passwords based on the default setting for username/password Security Level (Level 2, Maximum Security Checking).

Table 9-2: Username Examples

Valid	Invalid
Username Examples:	
fjohnson	fredj (too short)
fredj123	fred j 123 (contains spaces)
freDj-123	fj123 (too short)
fRedj-*123	fj 123 (contains spaces)
Password Examples:	
my-pa55word	my-pa55 (too short)
my-b1rthday	mybirthday (must contain numeric)
myd*g'snam3	mydogsnam3 (must contain a non-alphanumeric character)

Managing User Accounts

From the User List menu, you can complete the following tasks:

- Create an account
- Edit an existing account
- Change account passwords

The following figure shows the User List page:

Figure 9–1: User List Page



User Account Parameter Details

The configuration parameters for user accounts are provided in the following table.

Table 9–3: User Account Parameters





Detail	Description
TOS User Accounts	
Username	The login name used to access LSM management functions. Usernames must be 6 to 31 alphanumeric characters.
Access Level	The Distinguished Name of the Certificate Authority for this CA certificate.
Password Expiration	The Subject Distinguished Name entered when creating the request for this certificate the Create Certificate Requests page.
State	Whether the user account is currently disabled or enabled.
Function(s)  	<p>The functions available to manage the TOS User account:</p> <ul style="list-style-type: none"> • Delete the account. Only users with a Super-user security level can delete an account. • Edit the user account record to change the password, security level, and enable/disable the account. Only users with a Super-user or Administrator security level can modify another user's account. Operators can only modify their own account.

Table 9-3: User Account Parameters (Continued)

Detail	Description
Local Users	
Login	Username for the account. This is the login name used to access network services through the X family device. Usernames must be 6 to 31 alphanumeric characters.
Privilege Group	Privilege group which user account is a member of. This determines whether the user has VPN client access and if they are subject to firewall rule authentication and web filtering policies. For details, see “Privilege Groups” on page 253 .
Password Expiration	The number of days remaining until the password expires. When you create an account, the device uses the password expiration period configured from the Preferences page. For details, see “Preferences” on page 266 .
State	Whether the user account is currently disabled or enabled.
Function(s)  	The functions available to manage the Local User account: <ul style="list-style-type: none"> • Delete the account. Only users with a Super-user security level can delete an account. • Edit the user account record to change the password, security level, and enable/disable the account. Only users with a Super-user or Administrator security level can modify another user’s account. Operators can only modify their own account.

Create a New User Account in the TOS Authentication Database



Note Only a user with Super-user security level can create a user account.

STEP 1 From the LSM menu, select **Authentication > User List**.

STEP 2 Click **Create**.

STEP 3 Type a **Username**.

See [“Username and Password Requirements” on page 248](#) for more information.

STEP 4 Select a **User Type**:

- **TOS User** for administrators
- **Local User** for users that require access to network services.

STEP 5 Select the access level for the account:

- For TOS Users, select a **Security Level**: Operator, Administrator, Super-User.
- For Local Users, select a **Privilege Group**: Allow_VPN_Access or RADIUS. (For more information about privilege groups, refer to [“Privilege Groups” on page 253](#).)

STEP 6 Type a **Password**.

See [“Username and Password Requirements” on page 248](#) for more information.

STEP 7 Verify the password by re-entering it in **Confirm Password** field.

STEP 8 Click **Create**.

Change Your Password



Note All TOS users can change the password on their own account. Only users with Super-user access can change passwords on any account.

STEP 1 From the LSM menu, select **Authentication > User List**.

STEP 2 On the User List page, click your **Username**.

STEP 3 On the Edit User page, select the **Change Password** check box.

STEP 4 Type a **Password**.

See [“Username and Password Requirements” on page 248](#) for more information.

STEP 5 Verify the password by re-entering it in **Confirm Password**.

Enter the password exactly as you did in step 3.

STEP 6 Click **Save**.

How Local User Authentication Works: RADIUS, Privilege Groups and X.509 Certificates

Overview

Authentication on the X family device is an optional method of verifying the identity of a Local User and associating the user with privilege rights. Local users log into the device to access network services if the device has been configured to control access by user login (that is, the device has Local User accounts available for use).

On the X family device, authentication is used for the following purposes:

- Enable VPN client access for remote users, over a secure VPN tunnel (PPTP or L2TP)
- Provide firewall authentication, ensuring secure access to network resources between security zones
- Permit certain users to bypass web filtering

User authentication can also be implemented in conjunction with firewall rules, to restrict access to network services and applications.

The following explanation describes the authentication process, as implemented by the X family device.

- STEP 1** A user logs on to the device to gain access to network resources.
- To access network services through the device Firewall, the user opens up a standard Web browser and logs in using the LAN IP address of the device via HTTPS.
- When prompted, the user enters a username and password.
- STEP 2** The device authenticates the user (checks that the user is listed in the database and that the username and password are correct). Two methods are available for user authentication:
- Using a RADIUS authentication server. The preferred method, for large networks.
 - Using the local X family database. This can be used if no RADIUS server is available, typically for small networks.
- STEP 3** If no matching username and password can be located in the database, the firewall denies the login request.
- If a matching user is found, the firewall applies the privileges associated with the privilege group to which the user belongs.
- STEP 4** When a user requests a network service in another security zone, the device applies the relevant firewall rule for the type of service or application being requested:
- If a firewall rule is restricted to authenticated users and the user requesting the service is not in a privilege group that requires Firewall Rule Authentication, firewall rule matching skips to the next firewall rule in the table looking for a match.

For more detailed information on user authentication, refer to the *Concepts Guide*.

RADIUS

The X family supports user authentication via **Remote Authentication Dial-In User Service (RADIUS)**. Radius authentication may be used in place of the embedded user database within TOS, and may be used for all authenticated access for Local Users.

The following activities may be authenticated using RADIUS:

- VPN client dialup
- Inter-site VPN access
- Internet access
- Web filtering bypass

You can view and manage the RADIUS configuration parameters from the RADIUS page (**Authentication > Radius**).

Configure RADIUS

- STEP 1** From the LSM menu, select **Authentication > RADIUS**.
- STEP 2** On the RADIUS page, check **Enable RADIUS authentication** to use remote user authentication.
- STEP 3** To specify the activities managed by RADIUS authentication, check **User Authentication** and/or **VPN Client Access**.

You may choose to use RADIUS for VPN clients only, or to use it for both User Authentication and VPN Client Access.

STEP 4 In the **Radius Server Setup** table:

STEP A Type the **Server Timeout** value (between 1 and 30).

If no response is received from the RADIUS server, this value defines the time in seconds before the X family attempts to reconnect.

STEP B Type the **Server Retries** value (between 1 and 10).

This defines the number of times the X family will attempt to connect to the RADIUS server.

STEP 5 For the **Primary** and **Secondary RADIUS Servers**, type:

- **Address** — the IP/DNS address of the RADIUS server.
- **Port** — the UDP port number on the RADIUS server where you want X family to send the authentication requests. The default port number is 1812.
- **Shared Secret** — the password (between 8 and 128 characters) that you want the X family and RADIUS server to use for communicating with each other.
- **Authentication Method** — the protocol for authentication either **PAP** (Password Authentication Protocol) or **CHAP** (Challenge Handshake Authentication Protocol).

STEP 6 If the RADIUS server has not been configured with a Privilege Group attribute (Vendor Specific Attribute or VSA), select the **Default Privilege Group** to be assigned from the drop-down list.

STEP 7 Click **Apply**.

Privilege Groups

Privilege Groups allow you to setup access rights to specific services on the network that can then be enforced Firewall rules.

The types of global privileges that can be enabled for users within a group are:

- VPN client access
- Firewall rule authentication
- Web filter bypass

The Privilege Group is a component of the local user database entries or retrieved from RADIUS via a Vendor Specific Attribute (VSA). (For more information, see [“RADIUS” on page 252](#).) The device supports up to 100 Privilege Groups.

You can manage and configure from the Privilege Groups page. From this page you can:

- View currently configured Privilege Groups
- Delete a Privilege Group
- Create Privilege Groups

The following figures shows the Privilege Groups page.

Figure 9–2: Authentication: Privilege Groups Page



Privilege Group Parameter Details

The Privilege Groups page provides the following information:

Table 9–4: Privilege Group Information

Column	Description
Privilege Group	The name of the Privilege Group
VPN Client Access	Whether users in the group have VPN client dialup, inter-site VPN access or Internet access
Firewall Rule Authentication	Whether a user can bypass firewall rules configured for authentication
Web Filtering Bypass	Indicates whether users in the group can bypass firewall rules enforcing web filtering.
Function(s) ✗	<p>The available functions for Privilege Groups:</p> <ul style="list-style-type: none"> Delete a Privilege Group. To edit a Privilege Group, click the linked Privilege Group name in the Privilege Group List. <p>CAUTION You must delete the Privilege Group from any firewall rules with which it is associated before you delete the group.</p>

Create/Edit a Privilege Groups

- STEP 1** From the LSM menu, select **Authentication > Privilege Groups**. The Authentication - Privilege Groups page displays.
- STEP 2** On the Privilege Groups page, click the **Create Privilege Group** to add a Privilege Group, or click the linked **Privilege Group** name, to edit the Privilege Group. The AUTHENTICATION - Privilege Group (Create/Edit) page displays.

- STEP 3** On the **Create/Edit Privilege Group**, type or edit the **Privilege Group Name**. The name can be up to 32 alphanumeric characters, using only **a** to **z**, **A** to **Z**, **0** to **9**, **-** (hyphen) and **_** (underscore).
- STEP 4** Check or uncheck each of the following:
- **VPN Client Access** — allow/deny VPN client dialup, inter-site VPN access and Internet access.
 - **Policy Authentication** — allow/deny user authentication for firewall rules.
 - **Content Filter Bypass** — allow/deny user to bypass web filtering.
- STEP 5** Click **Create/Save** to save the changes and return to the Privilege Groups page. Click **Cancel** to return to the Privilege Groups page without saving the changes.

X.509 Certificates

Overview

The X family supports the use of X.509 certificates for VPN authentication and for secure management of your device. The use of certificates for verifying the identity of a device on the network for VPN is a more secure and scalable alternative to using a shared secret.

A certificate is a data file that is used to verify the identity of a device. The file contains unique information about the device, such as a Distinguished Name (DN), email address or domain name, which can be used to verify the identity of the device. The certificate links this identity to a public key value, which is also contained within the certificate.

Authentication depends on the integrity of the public key value in the certificate. The role of a certificate is to guarantee that the public key bound to the certificate can be used to verify the identity contained in the certificate.

To prevent users from tampering with public keys, all certificates must be signed by a certification authority (CA). A CA is a trusted source that confirms the integrity of the public key value in a certificate. This could be a CA server within an organization, or a public company like Verisign.

On the X family device, X.509 certificates are used for the following:

- Site-to-site VPN authentication
- Client-to-site VPN authentication

From the LSM, you can manage the following items required to perform authentication with X.509 Certificates:

- **CA Certificate** — Public certificate issued by a Certificate Authority. CA Certificates are used to validate received local certificates that were signed by this CA for other devices. The X family device supports the PKCS#7 or DER format for importing CA Certificates. An organization can install its

own CA server or use a third-party organization for creating certificates. The same CA certificate is imported onto all X family devices that must authenticate with each other.

- **Certificate Requests**—provides a form and encoding method for the X family administrator to generate a signed Local certificate from the CA server. The administrator has to export the Certificate Request, and then provide it to the CA server. The CA server signs the request to generate a Local Certificate and returns the signed certificate to the administrator who then imports it back into the X family device. A successful import of the Local Certificate removes the corresponding Certificate Request as the request has now been satisfied.
- A **Distinguished Name** uniquely identifies a certificate. The Distinguished Name is defined when creating the Certificate Request is used by the Local Certificate. The X family uses **PKCS#10 format** for Certificate Requests.
- **Local Certificates**—digitally signed certificates that are used to authenticate IPSec on the X family. Local Certificates are signed by a CA using a certificate request. The local certificate is a personal certificate, installed on the X family device or remote device. Each device has a unique local certificate. Other devices that have imported the CA certificate that was used to sign a local certificate can authenticate this device.
- **Certificate Revocation List (CRL)**— a list of certificates which have been revoked before their expiry dates by a Certificate Authority, along with the reasons for revocation and a proposed date for the next release. The Certificate Authority would revoke a certificate, for example, if there was a suspected compromise of the private part of public/private key pair that invalidates the public part, or if there was a change of user details.

Configuring X.509 Certificates

To use X.509 certificates as a secure method of authentication for VPN access to the network, you must configure both local and CA certificates before you configure other VPN services.

STEP 1 Import the CA certificate used to validate local certificates. For details, see [“CA Certificates” on page 257](#).

STEP 2 Create a Certificate Request and export it as a file that can be sent to the CA server. For details, see [“Certificate Requests” on page 260](#).

The CA server converts the request into a signed local certificate.

The local certificate is a personal certificate, installed on the X family device or remote device. Each device has a unique local certificate. The local certificate refers to the CA certificate for validation.



Note If you already have a local certificate with its own private key, you can import this certificate to the device from the Local Certificates page. It is not necessary to complete the Certificate Request process.

STEP 3 Import the signed local certificate retrieved from the CA server. For details, see [“Import a signed Local Certificate” on page 263](#).

STEP 4 To maintain the integrity of the CA certificates on the X family device, you can also associate a CRL with each certificate and configure parameters to automatically update the CRL. For details, see [“Certificate Revocation List \(CRL\) for a CA Certificate” on page 258](#).

For more detailed information on X.509 Certificates, see the *Concepts Guide*.

CA Certificates

CA Certificates are digital certificates issued and signed by either a local Certificate Authority server or a Certificate Authority organization such as Verisign. You can create CA Certificates and sign them yourself using tools like OpenSSL.

CA Certificates are installed on the CA server for your organization and are used to verify local certificates by signing them. The X family device supports the PKCS#7 or DER format for CA Certificates.

You can manage CA Certificates for the X family device from the LSM. From the CA Certificates page, you can:

- import the CA Certificates used by your organization
- view Current CA Certificates
- maintain a Certificate Revocation List (CRL) to ensure that the CA Certificates on the X family device are valid

The following figure shows the CA Certificate page.

Figure 9–3: Authentication: CA Certificate Page




Current CA Certificates Parameter Details

The **Current CA Certificates** table provides the following information about existing CA Certificates:

Table 9–5: Current CA Certificates Information

Column	Description
Name	Local name the device uses to reference the certificate, specified during the import process.
Expires On	Expiration date of the CA Certificate
Status	The status of the certificate, either: <ul style="list-style-type: none"> • Valid if the certificate may be used. • Revoked if the certificate has been revoked by a CRL.

Table 9–5: Current CA Certificates Information (Continued)

Column	Description
Functions   	For each CA Certificate listed in the table, you can: <ul style="list-style-type: none"> • Delete the certificate. • Export the certificate to a file. • Edit the CA Certificate to view the certificate details, specify a Certificate Revocation List (CRL), and configure parameters to automatically update the CRL.
CRL Expiry	The expiration date of the Certificate Revocation List (CRL) associated with the CA Certificate. This is set to No CRL loaded if the user has not configured a CRL for the CA
Status	The status of the certificate, either: <ul style="list-style-type: none"> • Valid if the certificate may be used. • Revoked if the certificate has been revoked by a CRL.

For additional information, see the following topics:

- [“X.509 Certificates” on page 255](#)
- [“Import a CA Certificate” on page 258](#)
- [“Configure CRL Parameters for a CA Certificate” on page 260](#)

Import a CA Certificate

STEP 1 From the LSM menu, select **Authentication > X.509 Certificates**.

STEP 2 On the CA Certificate page in the **Import CA Certificate** table, type a unique **Certificate Name** (for the name, use only characters: a-z, A-Z and 0-9 are allowed. (No spaces, symbols or special characters)

This is the local name that the X family device used to identify the CA Certificate in the LSM.

STEP 3 Type the path and file for the CA Certificate File, or click **Browse** and navigate to the file.

The CA Certificate file must use the .DER format (PKCS#7).

STEP 4 Click **Import** to upload the CA Certificate onto the X family.

After you import the CA Certificate, you can view and manage it from the **Current CA Certificates** table. To configure a CRL for the certificate, use the **Edit** function.

Certificate Revocation List (CRL) for a CA Certificate

The **Certificate Revocation List (CRL)** is a list of CA Certificates which have been revoked by a Certificate Authority before their expiration dates. The list includes the reasons for revocation and a proposed date for the next release. Certificates may be revoked because the private part of public/private key pair has been compromised, invalidating the public key, or if the user details for the certificate have changed.

Certificate Revocation Lists (CRLs) are continuously updated by the issuing Certificate Authority. To maintain the integrity of the CA Certificates, use the X.509 CA Certificate Details page to import and maintain the CRL used to validate the CA Certificate. From this page you can:

- View the certificate details
- Import a Certificate Revocation List (CRL) for the CA Certificate
- Configure automatic update of the CRL.

The following figure shows the X.509 CA Certificate Details page.

Figure 9–4: Authentication: X.509 Certificate Details Page

X.509 CA Certificates Parameter Details

The X.509 CA Certificate page provides the following information:

Table 9–6: CA Certificate Details

Detail	Description
Certificate Name	Name of the CA certificate.
Certificate Authority	The Distinguished Name of the Certificate Authority for this CA certificate.
Distinguished Name	The Subject Distinguished Name entered when creating the request for this certificate on the Create Certificate Requests page.
Certificate Serial Number	Serial number of this CA Certificate, shown in upper-case hexadecimal format.
Valid From	The start date of this CA Certificate, shown in the format <month> <day> <hour>:<min>:<sec> <year> <timezone>.
Expires On	The end date of this CA Certificate, shown in the format <month> <day> <hour>:<min>:<sec> <year> <timezone>.
CRL Expiry	Either the expiration date of the CRL associated with this CA Certificate, shown in the format <month> <day> <hour>:<min>:<sec> <year> <timezone>, or No CRL loaded if the user has not configured a CRL for the CA Certificate.

Configure CRL Parameters for a CA Certificate

- STEP 1** From the LSM menu, select **Authentication > X.509 Certificates**.
- STEP 2** On the CA Certificate page in the **Current CA Certificates** table, locate the CA Certificate that you want configure. Then, in the **Function(s)** field, click the **Edit** icon.
- STEP 3** On the X.509 CA Certificate Details page in the **Certificate Revocation List**, select **File**. Then, type the **File** path and name for the CRL, or click **Browse** and navigate to the file.
- STEP 4** Click **Import**.
- STEP 5** To configure the CRL for automatic update, select the **URL** radio button. Then:
- type the **URL** used to retrieve the CRL from the Certificate Authority.
 - type the **Update Interval** in hours. This specifies how often the device queries the CA website to check for updates.
 - Click **Set**.

Certificate Requests

Certificate Requests provide X family administrators with a form and encoding method to generate a signed Local Certificate from the CA server.

After generating the Certificate Request, the administrator has to export the request, and then provide it to the CA server. The CA server signs the request to generate a Local Certificate and returns the signed certificate to the administrator who then imports it back into the X family device. A successful import of the Local Certificate removes the corresponding Certificate Request as the request has now been satisfied. After importing a Local Certificate, you can view and manage it from the Local Certificates page.

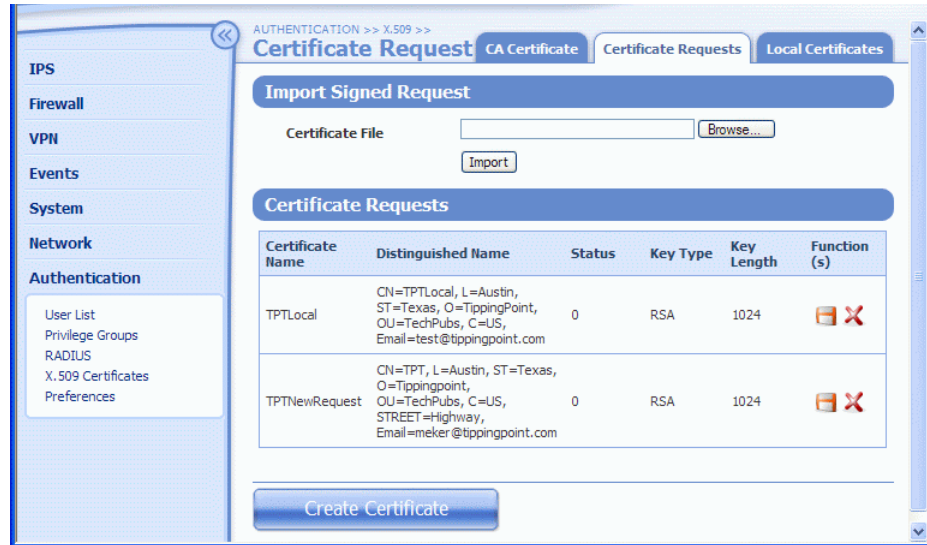
The device uses **PKCS#10 format** for Certificate Requests. When a request is created, a Distinguished Name (DN) and a public/private key pair is generated, and the public key is included in the PKCS#10 format.

You can manage Certificate Requests from the LSM. From the Certificates Request page, you can:

- View Certificate Requests currently available.
- Create a Certificate Request.
- Export the request so it can be submitted to the Certificate Authority.
- Import a signed Certificate Request that has been returned by the Certificate Authority so it is available for use on the system.

The following figure shows the Certificate Request page:

Figure 9–5: Authentication: Certificate Request Page



For additional information, see the following topics:

- [“Certificate Requests Parameter Details” on page 261](#)
- [“Managing Certificate Requests” on page 262](#)
- [“Import a signed Local Certificate” on page 263](#)
- [“X.509 Certificates” on page 255](#)

Certificate Requests Parameter Details

The Certificate Requests page provides the following information:



Table 9–7: Certificate Requests Details

Column	Description
Certificate Name	The name you gave to the Local Certificate when importing it.
Distinguished Name	The Distinguished Name of this Local Certificate. This is defined when you create the Certificate Request. The Distinguished Name is comprised of a number of attributes including: CommonName, Locale, State or Province, Organization, Department, Country, and Street Address.
Status	<p>The current status of the Certificate Request.</p> <ul style="list-style-type: none"> • Not Valid if the certificate is valid in the future, or if the authenticity cannot be verified using a CA certificate currently installed. • Valid if the certificate may be used • Revoked if the certificate has been revoked by a Certificate Revocation List (CRL)
Key type	Currently supports RSA as the type.
Key Length	Number of bits in the key, including 1024, 2048, 4096.

Managing Certificate Requests

You can perform the following management functions from the Certificate Request page:

Table 9–8: Certificate Request Functions

Function	Icon/Field	Description
Import Signed Local Certificate	Import Signed Request table	When you receive a signed certificate from the Certificate Authority, you can import the certificate so that it is available on the X family device. When you import a signed certificate from the Certificate Requests page, the certificate request generated to obtain the signed certificate is automatically deleted.
Create a Certificate Request	Create Certificate Request button	Access the Create a Certificate Request page to specify the parameters and Distinguished Name attributes for the request, and generate the Certificate Request in PKCS#10 format.
Export		A Certificate Request must be exported to a file before it can be submitted to the CA (either by a web-based service or by email). Certificate Requests are exported in PKCS#10 format , which includes the Distinguished Name (DN) and the Public Key. A request is signed by the Private Key of the requester so that the CA can verify authenticity.
Delete		If a Certificate Request is no longer needed, use the Delete function to remove it from the X family device. The device automatically deletes Certificate Requests when you import the signed local certificate received from the Certificate Authority.

For details, see the following sections:

- [“Create a Certificate Request” on page 262](#)
- [“Import a signed Local Certificate” on page 263](#)
- [“X.509 Certificates” on page 255](#)

Create a Certificate Request

- STEP 1** From the LSM menu, select **Authentication > X.509 Certificates**. On the CA Certificate page, click the **Certificate Requests** tab.
- STEP 2** On the Certificate Requests page, click **Create Certificate**.
- STEP 3** On the Create Certificate Request page, type a name for the Certificate Request in the **Name** field.

This is the name used by the Local Certificate when you later import the signed Local Certificate.
- STEP 4** Select the length for the private key from the **Length** drop-down list, either **1024 bits**, **1536 bits** or **2048 bits**.
- STEP 5** In the **Distinguished Name** table, define the Distinguished Name attributes for the Certificate Request:

STEP A In the **DN Attribute** field, select an attribute from the drop down list.

STEP B Type the value in the data field.

STEP C Click **Add to table below**.

The attribute and value are added to the Distinguished Name table. You can delete an attribute if required.

STEP D Repeat this process until you have defined the necessary information for the certificate.

STEP 6 Click **Create** to generate the Certificate Request in PKCS#10 format.

The Certificate Requests page displays with the generated request listed in the **Certificate Request** table.

After generating the request, use the **Export** function to save the file so you can submit the request to a Certificate Authority to obtain a signed local certificate.

Import a signed Local Certificate



Note Use this procedure to import the signed Certificate that you received from the Certificate Authority in response to submitting a Certificate Request generated from the LSM.

STEP 1 From the LSM menu, select **Authentication > X.509 Certificates**. On the CA Certificate page, click the **Certificate Requests** tab.

STEP 2 On the Certificate Requests page in the **Import Signed Request** table, type the **Certificate File** path and filename for the certificate request to import, or click **Browse** and navigate to the file.

This is the name of the signed Local Certificate file returned from the CA to which you transferred the Certificate Request file.

STEP 3 Click **Import**.

If the device verifies that the certificate can be trusted and that it matches a current **Certificate Request**, the certificate is imported. The matching certificate request is deleted. After the local certificate is imported, you can view and manage it from the Local Certificates page.

If the import fails, an error message explaining the failure is displayed.

Local Certificates

Local Certificates are used by X family device to authenticate IPSec on the device. Local Certificates are signed using the private key of a CA Certificate, which is a digital certificate issued by a Certificate Authority (CA).

The local certificate is a personal certificate, installed on the X family device or remote device. Each device has a unique local certificate. Because the local certificate has been signed by a CA, any other device that has imported and trusts the CA certificate can authenticate the X family device.

The device uses **PKCS#12 format** for importing Local Certificates with their private key. PKCS#12 format is a commonly used portable format for importing certificates into browsers. The imported file may also include the CA Certificate, in which case the device adds the CA Certificate to the CA list.

A local certificate can be installed using one of the following methods:

- Install the local certificate directly from the LSM Local Certificate page with a private key. With this method, you must know the private key and have a CA Certificate from the same Certificate Authority that signed the Local Certificate installed on the X family device.
- Perform the certificate request procedure from the LSM Certificate Requests page.

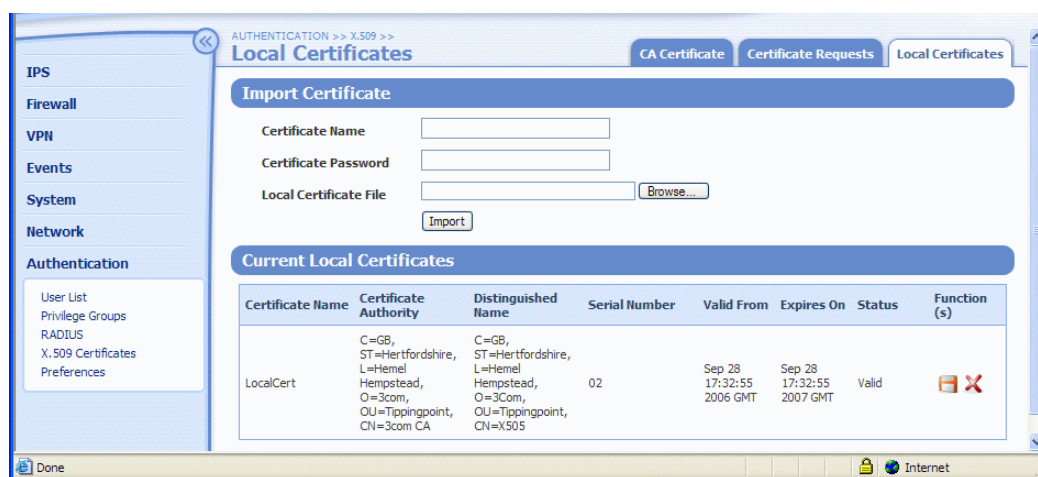
We recommend using the Certificate Request procedure because it is a more secure process. For details on the certificate request procedure, see [“Certificate Requests” on page 260](#).

You can manage Local Certificates from the Local Certificates Request page (**Authentication > X.509 Certificates, Local Certificates** tab). From this page, you can:

- View Local Certificates currently available
- Import a Local Certificate directly with a private key
- Export Local Certificates
- Delete Local Certificates

The following figure shows the Local Certificates page:

Figure 9–6: Authentication: X.509 Certificates: Local Certificates Page





Local Certificate Parameter Details

The **Current Local Certificates** table provides the following information about existing certificates:

Table 9–9: Local Certificate Details

Column	Description
Certificate Name	The name of the certificate
Certificate Authority	The Distinguished Name of the CA for this Local Certificate

Table 9–9: Local Certificate Details (Continued)

Column	Description
Distinguished Name	The Distinguished Name of this Local Certificate. See “Certificate Requests” on page 260 for information about Distinguished Names. These include CommonName, Locale, State or Province, Organization, Department, Country, and Street Address.
Serial Number	Serial number of this Local Certificate, shown in upper-case hexadecimal format
Valid From	The start date of this Local Certificate, shown in the format <month> <day> <hour>:<min>:<sec> <year> <timezone>
Expires On	The end date of this Local Certificate, shown in the format <month> <day> <hour>:<min>:<sec> <year> <timezone>
Status	The current status of this Local Certificate, either: <ul style="list-style-type: none"> • Valid • Revoked by CA CRL • Not Valid - certificate valid in the future • Not Valid - certificate has expired • Not Valid - unable to verify certificate with current CAs
Function(s)  	For each Local Certificate listed in the table, you can: <ul style="list-style-type: none"> • Delete the certificate. • Export the certificate to a file. You must provide the password for the certificate before you can export it.

For additional information, see the following topics:

- [“Create a Certificate Request” on page 262](#)
- [“Import a Local Certificate” on page 265](#)
- [“Export a Local Certificate” on page 266](#)

Import a Local Certificate

- STEP 1** From the LSM menu, select **Authentication > X.509 Certificates**. Then, select **Local Certificates**.
- STEP 2** On the Local Certificate page in the **Import Certificate** table, type a unique **Certificate Name**. Use only characters: only a-z, A-Z and 0-9 are allowed. (No spaces, symbols or special characters)
- This is the local name that the X family device used to identify the Local Certificate in the LSM.
- STEP 3** Type the **Certificate Password** for the Local Certificate.
- This password is issued by the Local Certificate provider.

- STEP 4** Type the **Local Certificate File** path and filename for the signed local certificate, or click **Browse** and navigate to the file.

The CA Certificate file must use the PKCS#12 format. You can only import a Local Certificate that has been signed by a CA Certificate available on the device. For details on importing CA Certificates, see [“CA Certificates” on page 257](#).

- STEP 5** Click **Import** to upload the Local Certificate onto the device.

If the import fails, an error message displays.

After you import the Local Certificate, you can view and manage it from the Current Local Certificates page.

Export a Local Certificate

- STEP 1** From the LSM menu, select **Authentication > X.509 Certificates**. Then, select **Local Certificates**.

- STEP 2** On the Local Certificates page in the Current Local Certificates page, click the Export icon for the certificate you want to export.

You must provide a valid password to export the Local Certificate.

- STEP 3** At the prompt, type the certificate password in the **Please enter the certificate password** field. Then, select **OK**.

- STEP 4** On the **File Download** dialog, click **Save**. Then, specify the path and filename to save the file.

Preferences

From the Preferences page on the Authentication menu, TOS users with a Administrative or Super-User access level can configure preferences to manage the security settings that affect TOS and Local User account access and session management and device session management.



TIP Session timeouts and password expiration periods may be covered in your company's information security policy. Consult your security policy to be sure you configure these values appropriately.

The following figure shows the Preferences page used to configure LSM user security settings:

Figure 9–7: Authentication - Preferences Page

The screenshot shows the 'Authentication - Preferences' page. The left sidebar has a tree view with 'Authentication' selected. The main panel has three sections: 'General User Preferences' with 'Web Idle Timeout' (60 minutes) and 'Page Refresh Time' (30 seconds); 'TOS User Preferences' with 'Security Level' (Maximum Security Checking), 'Password Expiration' (90 days), 'Password Expiration Action' (Force User to Change Password), 'Max Login Attempts' (5), 'Failed Login Action' (Lockout Account), and 'Lockout Period' (5 minutes); and 'Local User Preferences' with 'Inactivity Timeout' (10 minutes) and 'Maximum Session Time' (0 minutes). A 'Save' button is at the bottom.

Preferences Parameter Details

The following table provides information on the security preferences parameters.

Table 9–10: Authentication: Preferences for X Family User, Session, and Device Security

Field	Description
General User Preferences	
Web Idle Timeout	Amount of time (in minutes) that can elapse with no user activity before the LSM logs out account access. This setting prevents unauthorized users from accessing the LSM or X family services if the user is unexpectedly called away from the workstation or forgets to log out.
Page Refresh Time	Specify the time period for the Auto Refresh option available on pages that have dynamic content (such as the System Summary page, Log pages, and Health pages). If the option is enabled on a page, a countdown timer (starting with the value of Page Refresh Time) is started as soon as the page is opened. When the countdown expires, the page automatically refreshes.

Table 9–10: Authentication: Preferences for X Family User, Session, and Device Security (Continued)

Field	Description
TOS User Preferences	
Security Level	<p>Determines the length and complexity requirements for passwords. The following options are available:</p> <ul style="list-style-type: none"> • No Security Checking (Level 0)— Usernames cannot have any spaces. Passwords are not required. When this security level is selected, users must still enter a valid username to access the device or network services, but no password is required. • Basic Security Checking (Level 2)— User names must be between 6 and 32 characters long; passwords must be between 8 and 32 characters long. • Maximum Security Checking (Level 3)— User names must be between 6 and 32 characters long. <p>Passwords must be strong passwords, having 8 and 32 characters and containing at least one numeric character and one non-alphanumeric character (special characters such as ! ? and *). This is the default setting.</p>
Password Expiration	<p>Specifies how frequently users are required to change their passwords. You can disable this feature or select a time period (from 10 days up to 1 year) from the drop down list.</p> <p>TIP Best practices for password security recommend that password expiration periods should be a minimum of 30 days and maximum 90 days.</p>
Password Expiration Action	<p>Determines what action the device takes in response to a password expiration event. The following options are available:</p> <ul style="list-style-type: none"> • Force user to change the password when it expires. • Notify user of expiration. If this option is selected, the device notifies the user 5 days before the expiration occurs and at each subsequent login prompting the user to change the password before accessing the LSM. • Disable the account.
Max Login Attempts	Determines how many failed login attempts are allowed before the system takes the action specified in the Failed Login Action field.
Failed Login Action	<p>Determines what action the system takes when the Max Login Attempt count has been exceeded. The following options are available:</p> <ul style="list-style-type: none"> • Lockout Account. For this option, specify a Lockout Period. • Disable Account • Audit Event. This option creates an entry in the Audit log documenting the failed login attempt.
Lockout Period	If the Lockout Account is selected as the Failed Login Action, this value determines the duration of the lockout.

Table 9–10: Authentication: Preferences for X Family User, Session, and Device Security (Continued)

Field	Description
Local User Preferences	
Inactivity Timeout	For local users, the amount of time (in minutes) that can elapse with no user activity before the X family device logs out account access. This setting prevents unauthorized users from accessing network services if the user is unexpectedly called away from the workstation or forgets to log out.
Maximum Session Time	For local users, this value determines the maximum amount of time that the user can have access to authorized network services during one session.

Set User Preferences

STEP 1 From the LSM menu, select **Authentication > Preferences**.

The Preferences page displays with the current security settings. If the fields are read-only, your account does not have the required security access to edit the preferences. You must have an account with Administrator or Super-User access.

STEP 2 Change the values as desired. Then, click **Save**.

Browser Certificates

Details creating browser certificates for use in Internet Explorer to ensure notification messages are no longer reported to user.

Overview

Due to the security settings of the Local Security Manager (LSM), Internet Explorer may display a Client Authentication message followed by a Security Alert message. Message dialogs display when you first establish an HTTPS session with the X family device. This appendix details how to create certificates to remove these messages.

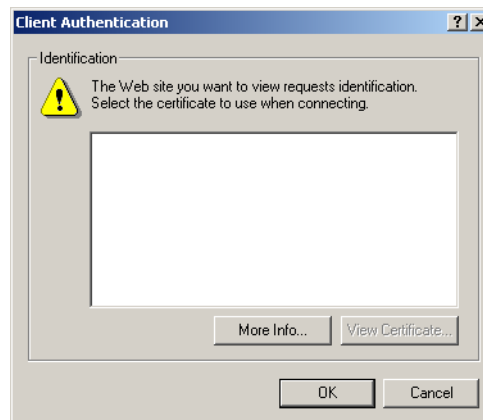
Browser Certificates includes the following sections:

- [“Client Authentication Message” on page 272](#)
- [“Security Alert” on page 273](#)
- [“Example - Creating Personal Certificate” on page 279](#)

Client Authentication Message

The X family device uses the same HTTPS channel to communicate with other products as it does to communicate with LSM. During the SSL handshake, the device asks for a client certificate for validation. This is meant for other products; however, LSM users may also be prompted for a client certificate. You can ignore this dialog.

Figure A-1: Client Authentication Dialog Box



To remove this warning, you can create and install a personal certificate on your workstation.

The following Procedures detail how to create and install the personal certificate:

- [“Creating a Personal Certificate” on page 272](#)
- [“Installing the Personal Certificate” on page 272](#)

Creating a Personal Certificate

The following command generates a self-signed certificate good for 10 years. The user must have access to a computer with OpenSSL installed on it. For the latest copy of OpenSSL, go to the OpenSSL web site: <http://www.openssl.org>.

STEP 1 Enter the following command:

```
openssl req -new -x509 -days 3650 -out cert.pem -keyout privkey.pem
```

This command creates two files: `cert.pem` and `privkey.pem`.

STEP 2 Enter the following command:

```
openssl pkcs12 -export -in cert.pem -inkey privkey.pem -out to_import.p12
```

This command creates the import file: `to_import.p12`.

Installing the Personal Certificate

The following instructions detail how to create the personal certificate. During the procedure, you will import the file called `to_import.p12`.

- STEP 1** Open Microsoft Internet Explorer (version 6.0 or later).
- STEP 2** Select **Tools > Internet Options**.
- STEP 3** Click on the **Content** tab. Click **Certificates**.
- STEP 4** Click **Import**. The **Certificate Import Wizard** opens.
- STEP 5** Click **Next**.
- STEP 6** On the File to Import screen, do the following:
- STEP A** Click **Browse**.
 - STEP B** Locate and select the file `to_import.p12`.
 - STEP C** Click **Next**.
- STEP 7** On the Password screen, do the following:
- STEP A** Enter your private key **Password**.
 - STEP B** Click the **Mark the private key as exportable** check box.
 - STEP C** Click **Next**.
- STEP 8** On the Certificate Store screen, select the option **Automatically select the certificate store based on the type of certificate**.
- STEP 9** Click **Next**.
- STEP 10** Click **Finish**. When the import completes, a message displays.

Security Alert

The Security Alert dialog in the following illustration shows two security alerts regarding certificates:

- [“Certificate Authority” on page 274](#) — The certificate is not from an trusted certifying authority
- [“Invalid Certificate Name” on page 277](#) — The name of the certificate is invalid

3Com creates a self-signed SSL device certificate for authentication with the browser. This allows X family devices to use SSL communication between the device and client web browser. This certificate may cause browsers to display a warning dialog, or to otherwise indicate the certificate is suspect. You can eliminate this dialog/warning by installing the certificate into the client certification trust list and placing an entry for the device in your local `HOSTS` or `LMHOSTS` file. The entry in the `HOSTS` file should name the host by its device serial number and then its IP address. This allows the SSL client to resolve the certificate common name.

Certificate Authority

The following dialog warning displays for a certificate authority security alert:

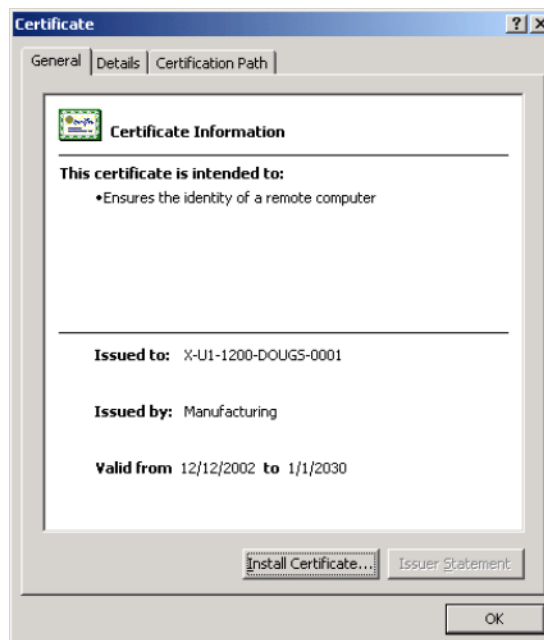
Figure A–2: Certificate Authority



You can eliminate the Certificate Authority warning with the following procedure:

STEP 1 When the warning displays, click **View Certificate**. The **Certificate** dialog box displays.

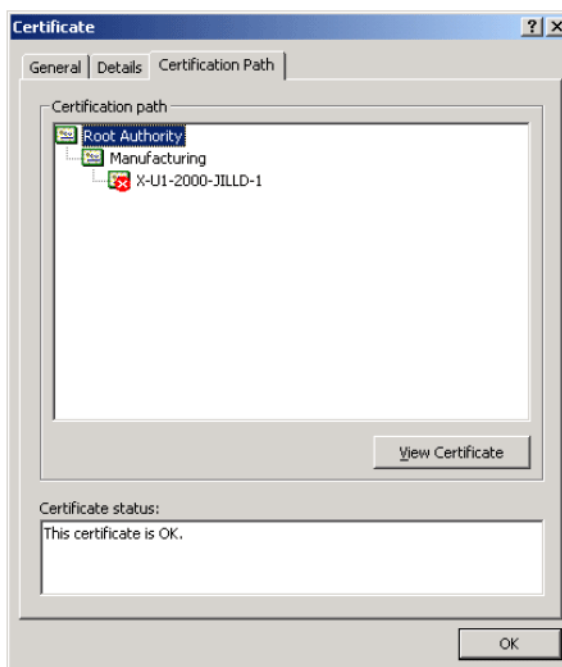
Figure A–3: Certificate Dialog Box



STEP 2 Select the **Certification Path** tab.

STEP 3 Select the **Root Authority**. Click **View Certificate**.

Figure A-4: Certification Path Tab - Root Authority



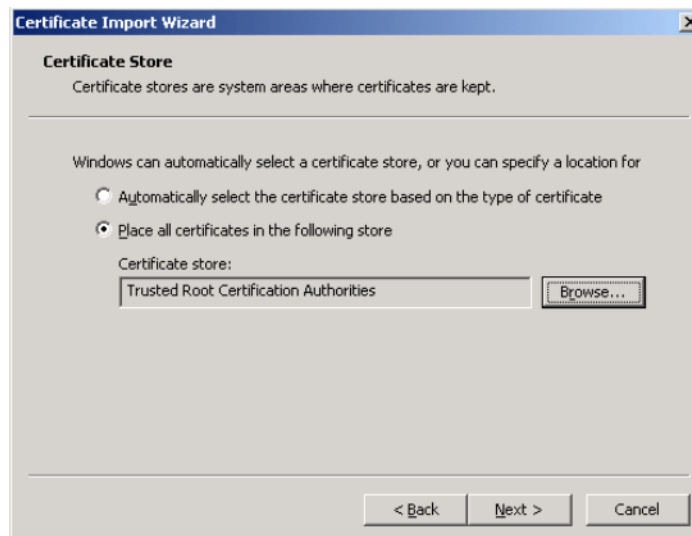
STEP 4 The Certificate Import Wizard opens. Click **Next**.

Figure A-5: Certificate Import Wizard



The **Certificate Store** dialog displays.

Figure A–6: Certificate Store Dialog



STEP 5 Select the **Place all certificates in the following store** option. The certificate store should be Trusted Root Certificate Authorities. Click **Next**.

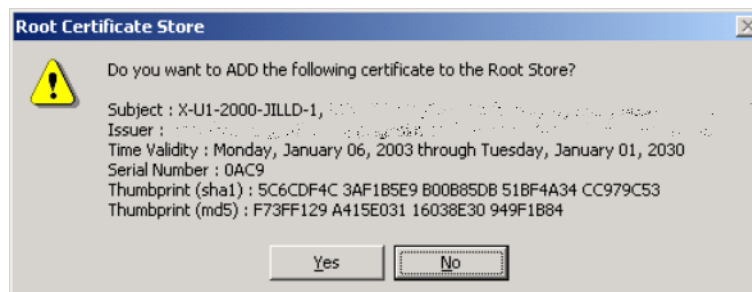
The Completing the Certificate Import Wizard dialog displays.

Figure A–7: Completing the Certificate Import Wizard Dialog



STEP 6 Click **Finish** to install the certificate. The Root Certificate Store indicates the status of the import and displays the certificate information.

Figure A-8: Root Certificate Store Verification



STEP 7 Click **Yes**. The X family device LSM login page displays.

Invalid Certificate Name

The following dialog warning displays for an invalid certificate name security alert:

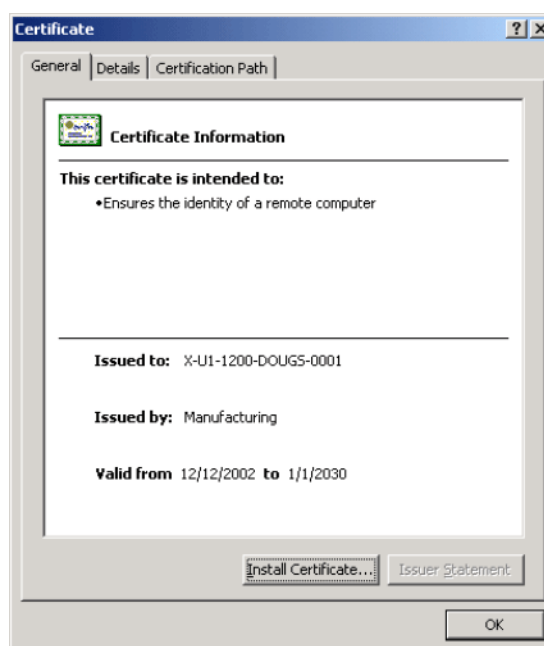
Figure A-9: Invalid Certificate Name



Performing the following steps can solve the Certificate Invalid warning:

STEP 1 When the warning displays, click **View Certificate**. The **Certificate** dialog box displays.

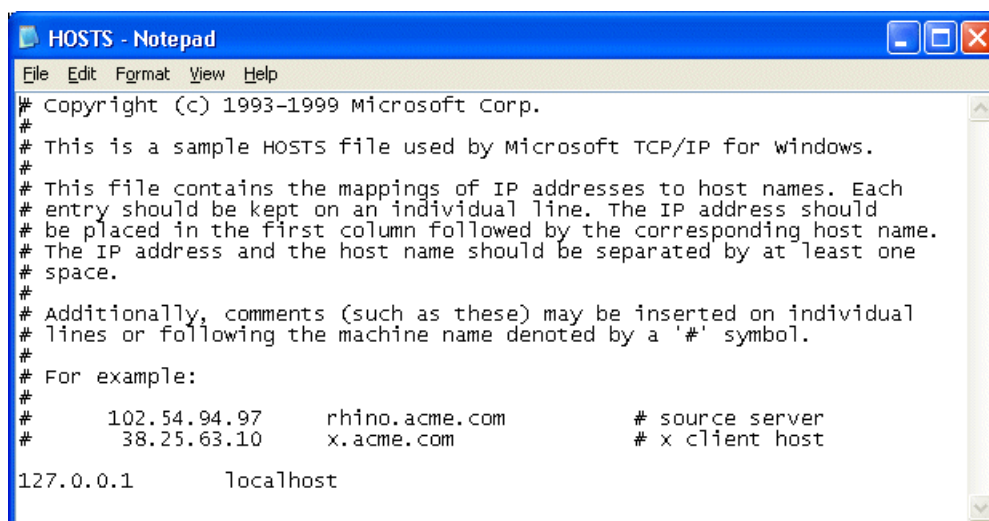
Figure A-10: Certificate Dialog Box



STEP 2 On the General tab, make note of the serial number.

STEP 3 Navigate and open the local workstation's HOSTS file. On a Windows XP system, this file is located in C:\WINDOWS\system32\drivers\etc.

Figure A-11: HOSTS File



STEP 4 Add a line to the file with the X family device's IP address and serial number.

- STEP 5** When browsing to the X family device, enter the workstation name instead of the IP address in your Web browser. This name and certificate works only on that particular workstation.

Example - Creating Personal Certificate

The following is an example of how to create you own personal certification. User entries are in bold. For security purposes, it is suggested that you do not use the passwords provided below.

```
[ ]# openssl req -new -x509 -days 3650 -out cert.pem -keyout
privkey.pem

Using configuration from /usr/share/ssl/openssl.cnf
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'privkey.pem'
Enter PEM pass phrase: DefaultPemPhrase
Verifying password - Enter PEM pass phrase: DefaultPemPhrase
-----

You are about to be asked to enter information that will be
incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name
or a DN.

There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----

Country Name (2 letter code) [GB]: US
State or Province Name (full name) [Berkshire]: Texas
Locality Name (eg, city) [Newbury]: Austin
Organization Name (eg, company) [My Company Ltd]: 3Com Corporation
Organizational Unit Name (eg, section) []: TAC
Common Name (eg, your name or your server's hostname) []: TPTI
Email Address []: my_email@3com.com
[ ]# openssl pkcs12 -export -in cert.pem -inkey privkey.pem -out
to_import.p12
Enter PEM pass phrase: DefaultPemPhrase
Enter Export Password: exportPassCode
Verifying password - Enter Export Password: exportPassCode
[ ]#
```


Web Filter Service

Detailed information about the Filter Service subscription service used to control access to web sites by categories. This service is offered in partnership with SurfControl, a market leading content filtering product.

Overview

The Web Filter Service is a subscription content filtering service that provides web content filtering based on web site category classifications. This service is operated in partnership with SurfControl, a provider of content filtering services.

On the X family device, all requests for web sites within a particular category are allowed or blocked depending on how the category is configured for the Web Filter Service. You can configure Web Filter Service category settings from the Web Filtering Service page (**Firewall > Web Filtering**) in the LSM. For details, see [“Web Filter Service” on page 90](#).

The Web Filter Service provides two main categories for filters:

- **Core Categories**

For details on what types of website are included in each core category, see [“Core Categories” on page 282](#).

- **Productivity Categories**

For details on what types of web sites are included in each productivity category, see [“Productivity Categories” on page 284](#).

In order to use the Web Filter Service, you need to purchase a license for the service. For details, see [“Purchasing a Web Filter License” on page 289](#).

Core Categories

Core Categories are used to classify web sites that contain offensive, potentially dangerous, or criminal content. On the X family device, all Core Categories are blocked by default. For information on the type of web sites included in each category, see the following topics:

- [“Adult/Sexually Explicit” on page 282](#)
- [“Criminal Skills” on page 282](#)
- [“Drugs, Alcohol & Tobacco” on page 282](#)
- [“Gambling” on page 283](#)
- [“Hacking” on page 283](#)
- [“Hate Speech” on page 283](#)
- [“Violence” on page 283](#)
- [“Weapons” on page 284](#)

Adult/Sexually Explicit

This Core category includes sites on the following topics:

- Sexually-oriented or erotic full or partial nudity depictions or images of sexual acts, including animals or other inanimate objects used in a sexual manner.
- Erotic stories and textual descriptions of sexual acts.
- Sexually exploitative or sexually violent text or graphics.
- Bondage, fetishes and genital piercing.
- Adult products including sex toys, CD-ROMs and videos.
- Adult services including video conferencing, escort services and strip clubs.
- Sexual health, breast cancer or sexually transmitted diseases (except in graphic examples) are not considered sexually explicit.

Criminal Skills

This Core category includes sites on the following topics:

- Advocating, instructing, or giving advice on performing illegal acts
- Tips on evading law enforcement
- Lock-picking and burglary techniques

Drugs, Alcohol & Tobacco

This Core category includes sites on the following topics:

- Recipes, instructions or kits for manufacturing or growing illicit substances including alcohol. These include purposes other than industrial usage sites that glamorize, encourage, or instruct on the use of or masking the use of alcohol, tobacco, illegal drugs or other substances that are illegal to minors.
- Alcohol and tobacco manufacturers' commercial Web sites.
- Sites detailing how to achieve ‘legal highs’, glue sniffing, misuse of prescription drugs or abuse of other legal substances.
- Sites that make available alcohol, illegal drugs, or tobacco free or for a charge displaying, selling, or detailing use of drug paraphernalia.
- Web sites discussing medicinal drug use, industrial hemp use, or public debate on the issue of legalizing certain drugs are not included in this Category Set. Nor are Web sites that are sponsored by

a public or private agency that provides educational information on drug use.

Gambling

This Core category includes sites on the following topics:

- Online gambling or lottery sites that invite the use of real money.
This also includes Web sites that provide phone numbers, online contacts or advice for placing wagers, participating in lotteries, or gambling real money newsgroups or sites discussing number running virtual casinos and offshore gambling ventures sports picks and betting pools.

Hacking

This Core category includes sites on the following topics:

- Promotion, instruction, or advice on the questionable or illegal use of equipment and/or software for purpose of hacking passwords, creating viruses, gaining access to other computers and/or computerized communication systems
- Sites that provide instruction or work-arounds for filtering software
- Cracked software and information sites; Warez
- Pirated software and multimedia download sites
- Computer crime

Hate Speech

This core category includes sites on the following topics:

- Web sites advocating or inciting degradation or attack of specified populations or institutions based on associations such as religion, race, nationality, gender, age, disability, or sexual orientation sites which promote a political or social agenda which is supremacist in nature and exclusionary of others based on their race, religion, nationality, gender, age, disability or sexual orientation.
- Holocaust revision/denial sites.
- Coercion or recruitment for membership in a gang or cult. A gang is defined as a group whose primary activities are the commission of felonious criminal acts, which has a common name or identifying sign or symbol and whose members individually or collectively engage in criminal activity in the name of the group. A cult is defined as a group whose followers have been deceptively and manipulatively recruited and retained through undue influence such that followers' personalities and behavior are altered. Leadership is all-powerful, ideology is totalistic and the will of the individual is subordinate to the group. A cult sets itself outside of society.
- News, historical, or press incidents that may include the above criteria (except in graphic examples) are not blocked.

Violence

This Core Category includes sites on the following topics:

- Web Sites portraying, describing or advocating physical assault against humans, animals or institutions.
- Depictions of torture, mutilation, gore or horrific death.
- Web Sites advocating suicide or self-mutilation.
- News, historical, or press incidents that may include the above criteria (except in graphic examples) are not blocked.

Weapons

This Core Category includes sites on the following topics:

- Instructions, recipes or kits for making bombs or other harmful or destructive devices.
- Web sites that primarily sell guns, weapons, ammunition or poisonous substances.
- Web sites that allow online purchasing or ordering information, including lists of prices and dealer locations.

Productivity Categories

Productivity Categories are used to classify web sites that could impair productivity when used in the work environment. On the X family device, all Productivity Categories are allowed by default.

Available Productivity Categories

This section provides a listing of the Productivity Categories available for the Web Filter Service. A description of the types of web sites included is provided for each category. Use the cross-references in the following table to locate information on a specific category.

The following table provides a list of the available Productivity Categories.

Table B–1: Web Filtering Service: Available Productivity Categories

Advertisement (see page 285)	Arts & Entertainment (see page 285)	Chat (see page 285)	Computing & Internet (see page 285)
Education (see page 285)	Finance & Investment (see page 286)	Food & Drink (see page 286)	Games (see page 286)
Glamour & Intimate Apparel (see page 286)	Government & Politics (see page 286)	Health & Medicine (see page 286)	Hobbies & Recreation (see page 287)
Hosting Sites (see page 287)	Job Search & Careers (see page 287)	Sites for Children (see page 287)	Lifestyle & Culture (see page 287)
Motor Vehicles (see page 287)	News (see page 287)	Personals & Dating (see page 287)	Photo Searches (see page 288)
Real Estate (see page 288)	Reference (see page 287)	Religion (see page 288)	Remote Proxies (see page 288)
Sex Education (see page 288)	Search Engines (see page 288)	Shopping (see page 289)	Sports (see page 289)
Streaming Media (see page 289)	Travel (see page 288)	Usenet News (see page 289)	Web-based Email (see page 289)

Advertisement

- Banner Ad Servers
- Pop-Up advertisements
- Adware

Arts & Entertainment

- Museums, galleries, artist sites (sculpture, photography, etc.)
- Performing arts (theatre, vaudeville, opera, symphonies, etc.)
- Dance companies, studios and training
- Book reviews and promotions, variety magazines and poetry
- Television, movies, music and video programming guides
- Online magazines and reviews on the entertainment industry
- Celebrity fan sites
- Broadcasting firms and technologies (satellite, cable, etc.)
- Horoscopes
- Jokes, comics, comic books, comedians or any site designed to be funny or satirical
- Online greeting cards
- Amusement/theme parks

Chat

- Web-based chat
- Instant Message servers



Note This category filters HTTP traffic only.

Computing & Internet

- Reviews, information, buyer's guides of computers, computer parts and accessories, and software
- Computer/software/Internet companies, industry news and magazines
- Pay-to-Surf sites

Education

- Educational institutions, including pre-, elementary, secondary, and high schools; universities
- Educational sites: pre-, elementary, secondary, and high schools; universities
- Distance education and trade schools, including online courses
- Online teacher resources (lesson plans, etc.)

Finance & Investment

- Web sites that provide stock quotes, stock tickers and fund rates.
- Web sites that allow stock or equity trading online.
- Investing advice or contacts for trading securities.
- Money management/investment services or firms.

Food & Drink

- Recipes, cooking instruction and tips, food products, and wine advisors
- Restaurants, cafes, eateries, pubs, and bars
- Food/drink magazines, reviews

Games

- Web sites that allow a user to download or play online games.
- Tips and advice on playing computer and Internet-based games.
- Journals and magazines dedicated to game playing.
- Web sites hosting games and contests.

Glamour & Intimate Apparel

- Lingerie, negligee or swimwear modeling.
- Supermodel fan pages.
- Fashion, clothing and glamour magazines or catalogues.
- Beauty and cosmetics.
- Fitness models and sports celebrities.
- Modeling information and agencies.

Government & Politics

- Local, state, federal and international government sites
- Government services such as taxation, armed forces, customs bureaus, emergency services
- Political parties
- Political debate, canvassing, election information and results
- Conspiracy theorist & alternative government views that are not hate-based

Health & Medicine

- Prescription medicines
- Medical information and reference about ailments, conditions, and drugs
- General health such as fitness and well-being
- Medical procedures, including elective and cosmetic surgery
- Dentistry, optometry, and other medical-related sites
- General psychiatry and mental well-being sites
- Psychology, self-help books, and organizations
- Promoting self-healing of physical and mental abuses, ailments, and addictions
- Alternative and complementary therapies, including: yoga, chiropractic and cranio-sacral
- Hospital, medical insurance

Hobbies & Recreation

- Recreational pastimes such as collecting, gardening, kit airplanes
- Outdoor recreational activities such as hiking, camping, rock climbing
- Tips or trends focused on a specific art, craft, or technique
- Online publications on a specific pastime or recreational activity
- Online clubs, associations or forums dedicated to a hobby
- Traditional (board, card, etc.) games and their enthusiasts
- Animal/pet related sites, including breed-specific sites, training, shows and humane societies

Hosting Sites

Web sites that host business and individuals' web pages (i.e. GeoCities, earthlink.net, AOL)

Job Search & Careers

- Sites hosting job and resume listings.
- Tips and strategies for job seekers and interviewees.
- Online job finding services.

Sites for Children

Child oriented sites and sites published by children

Lifestyle & Culture

- Home life and family-related topics, including weddings, births and funerals
- Parenting tips and family planning
- Gay/lesbian/bisexual (non-pornographic) sites
- Foreign cultures, socio-cultural information
- Tattoo, piercing parlors (non-explicit)

Motor Vehicles

- Car reviews, vehicle purchasing or sales tips and parts catalogues.
- Auto trading, photos, discussion of vehicles including motorcycles, boats, cars, trucks and RVs.
- Journals and magazines on vehicle modification, repair or customization.
- Online automotive enthusiast clubs.

News

- Online newspapers.
- Headline news sites.
- News wire services.
- Personalized news sources.

Personals & Dating

- Web sites that provide singles listings.
- Matchmaking and dating services.
- Advice for dating or relationships.
- Romance tips and suggestions.

Photo Searches

- Sites that provide resources for photo and image searches
- Online photo albums/digital photo exchange
- Image hosting

Real Estate

- Home, apartment, and land listings.
- Rental or relocation services.
- Tips on buying or selling a home.
- Mortgage and home loan information.
- Home improvement.
- Real estate agents and agencies.

Reference

- Personal, professional, or educational reference
- Online dictionaries, maps, and language translation sites
- Census, almanacs, and library catalogues
- Topic-specific search engines

Religion

- Churches, synagogues, and other houses of worship
- Any faith or religious beliefs, including non-traditional religions such as Wicca and witchcraft

Remote Proxies

- Remote proxies or anonymous surfing
- Search engine caches that circumvent filtering
- Web-based translation sites that circumvent filtering

Sex Education

- Pictures or text advocating the proper use of contraceptives
- Sites relating to discussion about the use of the Pill, IUDs and other types of contraceptives
- Discussion sites on how to talk to your partner about diseases, pregnancy and respecting boundaries



Note Not included in the category are commercial sites that sell sexual paraphernalia. These sites are typically found in the Adult category.

Search Engines

General search engines (Yahoo, AltaVista, Google)

Shopping

This Productivity category includes sites on the following topics:

- Internet malls and online auctions.
- Department stores, retail stores, company catalogs online.
- Online downloadable product warehouses; specialty items for sale.
- Companies online dedicated to freebies or merchandise giveaways.

Sports

This Productivity category includes sites on the following topics:

- Official team or conference Web sites.
- National, international, college, professional scores and schedules.
- Virtual sports leagues and teams.
- Sports-related online magazines or newsletters.

Streaming Media

- Streaming media files or events (any live or archived audio or video file)
- Internet TV and radio
- Personal (non-explicit) webcam sites
- Telephony sites that allow users to make calls via the Internet
- VoIP services

Travel

This Productivity category includes sites on the following topics:

- Airlines and online flight booking agencies.
- Accommodation, information and weather bureaus.
- Leisure travel package listings.
- Tourist information and maps.

Usenet News

This blocks access to newsgroups accessed through the http protocol.

Web-based Email

- Web-based e-mail accounts
- Messaging sites (SMS, etc.)

Purchasing a Web Filter License

The Web Filter Service is a subscription-based service which requires the purchase of the correct license for your product from a reseller.



Note: You do not have to purchase a license to filter web sites using the Custom Filter List.

Each license allows one year of filtering for a specific X family product. Licenses cannot be transferred between base products, except through the standard Return Materials Authorization (RMA) process.

When you purchase a Web Filter Service subscription, you will receive a License pack which includes a unique License Key. To enable the Web Filter Service for your product, register the License Key at <http://eSupport.3com.com>. You also need to provide the serial number of the specific X family device for which you are enabling the service.



Note: The purchase of a Web Filter Service license does not extend any warranties or support contracts on the base product.

Free 14-day Trial Period

When you receive a new X family device, you can sign up for a 14-day trial period for the Web Filter Service. During the trial period, you do not need a license for the service. The trial period is activated when you register the device.



Log Formats and System Messages

Details the formats of the downloadable logs and system update status messages.

Overview

This appendix contains information on the formats of each of the downloaded logs from the Local Security Manager (LSM). This includes information on the remote syslog format and High Availability messages contained in the System Log. This chapter describes messages received during the system update process.

- [“Log Formats” on page 292](#)
 - [“Alert and IPS Block Log Formats” on page 292](#)
 - [“Audit Log Format” on page 294](#)
 - [“Firewall Block Log Format” on page 296](#)
 - [“Firewall Session Log Format” on page 298](#)
 - [“VPN Log Format” on page 299](#)
 - [“System Log Format” on page 300](#)
- [“Remote Syslog Log Format” on page 301](#)
- [“High Availability Log Messages” on page 302](#)
- [“System Update Status Messages” on page 303](#)

Log Formats

In the LSM, you can view all the logs in the GUI. In addition, you can download a text-only version of the log and view it in a browser window or save it in a file. If you save a log in a file, you can then off load it to a remote syslog server. When downloading a log, the format is a stream of data separated by the delimiter specified in the GUI.

In the System Log, the fields displayed in the GUI are the same as the fields in the downloaded log. In the other five logs, the fields that are shown in the GUI are only a subset of what is available in the downloaded log file.

This section documents the fields that are in the downloaded versions of these logs. These field definitions are helpful when reading the downloaded log file. They contain the description of the data so that you can format the desired fields in a reporting program such as Excel or Access, or send it to a remote syslog server.

Delimiters

In the LSM GUI, on the Download Log page, you can specify one of the following delimiter formats:

- **tab** (This is the default.) The field names do not appear on the tab delimited format.
- **comma** (csv)

For both types of delimiters, the sub-fields within the **Message** field are always tab delimited. If a Message sub-field is not used a tab is inserted to move onto the next sub-field.

Alert and IPS Block Log Formats

An example of a comma-delimited IPS Block Log entry follows:

```
1, 2006-08-22 16:31:39,INFO,BLK,"Block v4 2 [3f937e55-31e9-11db-9452-0800179bd3a4] 1 [00000001-0001-0001-0001-000000000164] icmp 0
192.168.1.1:0 209.191.93.52:0 1 0 0 [cc2f252a-1a57-4d00-8dc8-a34e69992c46] ANY [cc2f252a-1a57-4d00-8dc8-a34e69992c46] ANY
1156260699 0000000000 1 pt0 0 0 0 0324"
```

The following table describes the downloadable format of the Alert Log and IPS Block Log:

Table C-1: Alert and IPS Block Log Formats

Field Name	Sub-Field Name	Description
Seq		Unique sequence number for this log file.
Entry_time		Date and time of event. YYYY-MM-DD 24H:MI:SS
Sev		Severity of the alert, from least to most severe: <ul style="list-style-type: none"> • INFO = for information only • WARN = warning • ERR= error • CRIT = critical

Table C–1: Alert and IPS Block Log Formats (Continued)

Field Name	Sub-Field Name	Description
Comp		Software component that generated the message: <ul style="list-style-type: none"> • ALT = Alert Log • BLK = IPS Block Log
Message (Contained within quotes.)	Alert Action	<ul style="list-style-type: none"> • Alert = for Alert Log • Block = for IPS Block Log
	Policy Log Version	v4
	Alert Type	A bit field that identifies a message as traffic threshold, invalid, etc.
	Policy UUID	ID for the policy, enclosed within brackets ([]). Default policies begin with “[00000002-...”
	Message Severity	1 = low 2 = minor 3 = major 4 = critical
	Signature UUID	Signature ID from the DV, enclosed within brackets ([]). Can you have multiple policies per signature. Default signatures begin with “[00000001-...”
	Protocol	Protocol of the alert. Examples: HTTP, IP, TCP, UDP, and ICMP.
	IP Protocol Numeric	Layer 2 protocol (uint). Only used in Firewall Block Logs for the X family device. In all other logs, this field will be 0.
	IP Protocol String	Layer 2 protocol (string). Only used in Firewall Block Logs for the X family device. In all other logs, this field will be blank.
	Source IP Address and Port	Packet's source IP address and port. Format is <address>:<port>
	Destination IP Address and Port	Packet's destination IP address and port. Format is <address>:<port>
Message (continued)	Hit Count	The aggregated number of messages received.
	In MPHY	Physical port number in which the packet arrived.
	VLAN	(int)
	In Security Zone UUID	(uuid)

Table C–1: Alert and IPS Block Log Formats (Continued)

Field Name	Sub-Field Name	Description
	In Security Zone NAME	(string) Example: ANY
	Out Security Zone UUID	(uuid)
	Out Security Zone NAME	(string) Example: ANY
	Date & Time (Seconds)	Beginning timestamp, in seconds, of the aggregation period.
	Date & Time (Nanoseconds)	Beginning timestamp, in microseconds, of the aggregation period.
	Period	Aggregation period, in minutes. 0 = no aggregation.
	Message Parameters	A string of values for special message formats used for traffic thresholds. This value is usually blank.
	Packet Trace Log Flag	Packet trace flag/version. • pt0 = off • pt1 = on
	Packet Trace Bucket ID	Packet trace aggregation bucket sequence number.
	Packet Trace Sequence Begin	Packet trace aggregation bucket beginning sequence number.
	Packet Trace Sequence End	Packet trace aggregation bucket ending sequence number.
	Number of characters in the line	This is used for reverse parsing of the entry.

Audit Log Format

An example of a comma-delimited Audit Log entry follows:

```
48,2006-08-04 12:46:11,8,CLI,0.0.0.0,LCD,0,0,labuser,"Created policy rule 100"
```

The following table describes the downloadable format of the Audit Log:

Table C–2: Audit Log Format

Field Name	Description
Seq	Unique sequence number for this log file.

Table C-2: Audit Log Format (Continued)

Field Name	Description
Entry_time	Date and time of event. YYYY-MM-DD 24H:MI:SS
Access	The access-level of the user performing the action.
Type	The interface from which the user logged in. <ul style="list-style-type: none"> • WEB for the LSM • CLI for the Command Line Interface
Address	The IP address from which the user connected to perform the action.
Cat	The area in which the use performed an action (LOGIN, LOGOUT, and Launch Bar tabs).
Result	<ul style="list-style-type: none"> • 0 = Pass • 1 = Fail
Flag	Not used.
User	The login name of the user performing the action. The user listed for an event may include SMS, SYS, and CLI. These entries are automatically generated when one of these application performs an action.
Message (Contained within quotes.)	The message text associated with the event. The action performed as a result; for example, Log Files Reset.

Firewall Block Log Format

An example of a comma-delimited Firewall Block Log entry follows:

```
6,2006-10-05 17:12:31,INFO,BLK,"Block v4 2 [c52e3da9-23e0-11db-9cdd-00132055ccd2] 1 [00000001-0001-0001-0001-000000007400] firewall 17 UDP
152.67.137.49:137 152.67.140.3:137 1 0 0 [e3d4586b-67a6-4662-bc17-560455bedf54] LAN [08585a5d-23e1-11db-9cdd-00132055ccd2] MGMT
1160086351 0587833079 1 1 0 | | | pt0 0 0 0 0344"
```

The following table describes the downloadable format of the Firewall Block Log:

Table C-3: Firewall Block Log Format

Field Name	Sub-Field Name	Description
Seq		Unique sequence number for this log file.
Entry_time		Date and time of event. YYYY-MM-DD 24H:MI:SS
Sev		Severity of the alert, from least to most severe: <ul style="list-style-type: none"> • INFO = for information only • WARN = warning • ERR = error • CRIT = critical
Comp		Software component that generated the message. Example: BLK.
Message (Contained within quotes.)	Action	
	Version	
	AlertType	
	Policy UUID	The UUID of the Firewall Rule that matched.
	Severity	Not used.
	Signature UUID	Not used.
	Protocol Type String	String name of the Protocol field (e.g. "tcp").
	Protocol Number	The IP protocol number used for the session by the starter.
	Protocol Name	String name of the Protocol (e.g. "http")
	Source IP	The source IP address and port for the session. This represents the "starter" of the session. Format is ddd.ddd.ddd.ddd:port.

Table C-3: Firewall Block Log Format (Continued)

Field Name	Sub-Field Name	Description
Message (cont.)	Destination IP	The destination IP address and port for the session. This represents the “target” of the session. Format is ddd.ddd.ddd.ddd:port.
	Packets Delta	Not used.
	Mphy	Ingress Port Number.
	Vlan	Ingress VLAN. Normally used to identify the Security Zone.
	Source Zone UUID	The UUID for the zone on which the source IP address appears.
	Source Zone Name	The zone on which the source IP address appears.
	Destination Zone UUID	The UUID for the zone on which the destination IP address appears.
	Destination Zone Name	The zone on which the destination IP address appears.
	Start time Secs	Unused by Firewall. UDM Log Aggregation.
	Start time Nanosecs	Unused by Firewall. UDM Log Aggregation.
	Period	Unused by Firewall. UDM Log Aggregation.
	Message Params	<p>The Message Params are further delimited as using the ‘ ’ character as follows:</p> <ul style="list-style-type: none"> • FirewallRuleId: The customer visible firewall rule id that matched (allowed) the session to go through. By definition this is a Permit rule. This should match the Policy UUID. • Category: For web requests that were filtered by the Web Filter Subscription Service, the category that the URL field was matched to. • URLInfo: For web requests, this is the extra information from web filter engine for block decision. • URL For web requests, the target URL. This field is filled in regardless of whether the request was filtered by the Web Filter Subscription Service. <p>When the Log is being saved through the LSM, the fields in Message Params are exported with tab separation (blanks for unused fields) to allow easy import into Excel.</p>
	Packet trace flag	Packet trace not supported by Firewall.

Table C–3: Firewall Block Log Format (Continued)

Field Name	Sub-Field Name	Description
Message (cont.)	Packet trace seq begin	Packet trace not supported by Firewall.
	Packet trace seq end	Packet trace not supported by Firewall.

The fields in this table are populated depending on the event being logged:

- **Block event:**

This event represents a firewall block. The Category, URL, Session Start and Bytes fields will be blank. The Firewall Rule field should be a hyperlink to the Firewall Rule edit page.

- **Web Filter Block Event:**

This event is generated for a Web request that is blocked by the box. All specified fields are provided. The category field will be populated if the Web request was blocked by the Web Filter Subscription service (not for a manual URL block).

Firewall Session Log Format

An example of a comma-delimited Firewall Session Log entry follows:

```
87148 2006-10-23 20:26:07 INFO TNT 75.121.191.83:4672
190.206.247.84:4672 17 UDP(17) e3d4586b-67a6-4662-bc17-560455bedf54
LAN 0dc7c57b-4ff9-467f-8ef6-d5069850a1c6 WAN 100
Regular Session Start
```

The following table describes the downloadable format of the Firewall Session Log:

Table C–4: Firewall Session Log Format

Field Name	Description
Seq	Unique sequence number for this log file.
Entry_time	Date and time of event. YYYY-MM-DD 24H:MI:SS
Sev	Severity of the alert, from least to most severe: <ul style="list-style-type: none"> • INFO = for information only • WARN = warning • ERR= error • CRIT = critical
Comp	Software component that generated the message. Examples: GEN, TNT
SrcIP	The source IP address and port for the session. This represents the “starter” of the session. Format is ddd.ddd.ddd.ddd:port.

Table C-4: Firewall Session Log Format (Continued)

Field Name	Description
DstIP	The destination IP address and port for the session. This represents the “target” of the session. Format is ddd.ddd.ddd.ddd:port.
Protocol Number	
Protocol	<protocol name> (<protocol number>)
Source Zone UUID	The UUID for the zone on which the source IP address appears.
Source Zone Name	The zone on which the source IP address appears.
Destination Zone UUID	The UUID for the zone on which the destination IP address appears.
Destination Zone Name	The zone on which the destination IP address appears.
Firewall Rule ID	The firewall rule id that matched (allowed) the session to go through. By definition this is a Permit rule.
Category	For Web requests that were filtered by the Web Filter Subscription Service: the category to which the URL field was matched.
URL	For Web requests: the target URL. This field is populated regardless of whether the request was filtered by the Web Filter Subscription Service.
Session Duration(s)	For Session End Events only: this field contains the duration of the session from its start time in DD:HH:MM.SS format.
Bytes	For Session End Events only: this field contains the number of bytes transferred during the session.
Message	The message text associated with the event.

VPN Log Format

An example of a comma-delimited VPN Log entry follows:

```
17,2006-10-05 17:12:31,INFO,VPN,"152.67.137.49:500 10.171.2.254:500
Responder started IKE phase 1, main mode"
```

The following table describes the downloadable format of the VPN Log:

Table C-5: VPN Log Format

Field Name	Description
Seq	Unique sequence number for this log file.
Entry_time	Date and time of event. YYYY-MM-DD 24H:MI:SS

Table C–5: VPN Log Format (Continued)

Field Name	Description
Sev	Severity of the alert, from least to most severe: <ul style="list-style-type: none"> • INFO = for information only • WARN = warning • ERR= error • CRIT = critical
Comp	Software component that generated the message: VPN.
Message (Contained within quotes.)	The message text associated with the event.

System Log Format

An example of a comma-delimited System Log entry follows:

```
21,2006-08-04 12:43:29,ERR ,DRV,"No cryptonet devices found."
```

The following table describes the downloadable format of the System Log:

Table C–6: System Log Format

Field Name	Description
Seq	Unique sequence number for this log file.
Entry_time	Date and time of event. YYYY-MM-DD 24H:MI:SS
Sev	Severity of the alert, from least to most severe: <ul style="list-style-type: none"> • INFO = for information only • WARN = warning • ERR= error • CRIT = critical
Comp	Software component that generated the message. Examples: SYS, UDM, and HTP.
Message (Contained within quotes.)	The message text associated with the event. For a list of High Availability messages, see section “High Availability Log Messages” on page 302 .

Remote Syslog Log Format

The remote syslog format for the Alert, IPS Block, and the Firewall Block Logs is described in this section.



Note For the System, Audit, VPN, and Firewall Session Logs, there is no specific format for the remote syslog. For these logs, the downloaded file is sent directly to the remote syslog server as a straight data dump without any manipulation of the data.

The following is an example of packet data sent to a collector. Make note that collectors may display the header portion of the stream differently.

```
<13>Jan 13 12:55:01 192.168.65.22 ALT,v4,20050113T125501+0360,"i
robot"/192.168.65.22,1017,Alert,1,1,00000002-0002-0002-0002-
000000000164,"0164: ICMP: EchoRequest (Ping)","0164: ICMP: Echo
Request (Ping)",icmp,0,216.136.107.233:0,216.136.107.91:0,20
050113T125205+0360,199," ",1,3:1
```

In this example, the header follows the standard syslog format. Using the previous log entry as the example, the message is as follows:

```
ALT,v4,20050113T125501+0360,"i robot"/
192.168.65.22,1017,Permit,1,Low,00000002-0002-0002-0002-
000000000164,"0164: ICMP: EchoRequest (Ping)","0164: ICMP: Echo
Request (Ping)",icmp,0,216.136.107.233:0,216.136.107.91:0,20050113T1252
05+0360,199," ",1,3:1
```

The character located between each field is the configured delimiter. In this case, the delimiter is a comma. The following table details the fields and their descriptions.

Table C-7: Remote Syslog Field Descriptions

Field	Description
1	Log-type; ALT = alert, BLK = block, P2P = misuse and abuse
2	Version of this message format
3	ISO 8601 Date-Time-TZ when this alert was generated
4	Hostname/IP address that generated the alert; note that the quotes are required for this release because of a bug in the hostname validation (note the space in the name)
5	Sequence ID
6	(reserved)
7	Action performed ("Block" or "Permit")
8	Severity ("Low", "Minor", "Major", or "Critical")
9	Policy UUID

Table C–7: Remote Syslog Field Descriptions (Continued)

Field	Description
10	Policy Name
11	Signature Name
12	Protocol name (“icmp”, “udp”, “tcp”, or “unknown”)
13	Firewall IP Protocol Numeric and String. Format is <code><uint> (<string>)</code> . Only used in Firewall Block Logs for the X family device. In all other logs, this field will be 0.
14	Source address and port, colon delimited
15	Destination address and port, colon delimited
16	ISO 8601 Date-Time-TZ when the aggregation period started
17	Number of events since start of aggregation period
18	Traffic Threshold message parameters
19	Traffic capture available on device (available = 1; none = 0)
20	Slot and segment of event

High Availability Log Messages

The High Availability mechanism logs the following messages to the System Log. For details on the System Log, see [“System Log Format” on page 300](#).

Table C–8: High Availability Log Messages

Message	Type	Description
Changed to HA active state	Informational	Standby device has determined that active device is not responding to HA polling or has been manually forced to active state
Changed to HA standby state	Informational	Active device has determined that it should return to standby state or has been manually forced to standby state
Active HA device (ip-address) detected	Informational	Standby device has detected one of the HA management IP addresses of the active device. This should be logged for each of the IP interfaces that is configured with an HA management IP address.

Table C–8: High Availability Log Messages (Continued)

Message	Type	Description
Standby HA device (ip-address) detected	Informational	Active device has detected one of the HA management IP addresses of the standby device. This should be logged for each of the IP interfaces that is configured with an HA management IP address.
Active HA device (ip-address) requesting pre-emption	Informational	Active device has detected that other device is also active (e.g. manually forced to active) and should return to standby.
Active HA device (ip-address) no longer detected	Warning	Standby device has determined that the active device is not responding to the HA heartbeat mechanism on one of the HA management IP addresses.
Standby HA device (ip-address) no longer detected	Warning	Active device has determined that the standby device is no longer polling it on one of the HA management IP addresses.

System Update Status Messages

The LSM provides update status on the progress of the update. The messages include “<Update State>:<qualifier>”. The <Update State> indicates the state of the update. The <qualifier> provides information about the state. The following table details the messages that display on the LCD screen during an update of the TOS:

Table C–9: IPS Update States

Update State	Description
Ready	Device is ready for an update.
Updating	Device is in the process of updating.
UpdateCommitting	Device has rebooted and is processing the final update steps.
UpdateFailure	Device failed Update. The screen displays the reason.
Rollback	Device is in the process of rollback.
RollbackCommitting	Device has rebooted and is processing the final rollback steps.
RollbackFailure	Device failed Rollback. The screen displays the reason.
Failsafe	Device was unable to load a valid image and is running a scaled-back image.

If an error occurs, the information changes. The state displays as “UpdateFailure:<state>” where <state> is one of the listed states in the previous table. The listed state displays a qualifier and message regarding the state. The following table details the qualifier and messages:

Table C–10: IPS Update Failure Messages

Update Failure Qualifier	Message
OK	Normal operation, no errors
InvalidUpdateState	Current action is restricted while device is in this state. Fix problem and reset Update State.
InvalidLocation	Package file not found at that location.
RebootDuringUpdate	Device was rebooted during update. Check system log for recommendations.
TarChecksumError	Checksum error when extracting the archive: Corrupted package.
TarExtractError	File system error when extracting the archive.
ArchiveCreateFailure	File system error creating rollback archive.
SystemError	General error during update.
WrongPlatformType	Package is for a different platform. Make sure you have correct IPS package.
PackageReadError	General error while reading package. Possible Truncated or Corrupted package, download new package from TMC and retry update.
WrongPackageType	Package is of unknown type, not an OS or DV package. Make sure you have correct IPS package.
NotEnoughFreeSpace	Not enough available disk space. Remove older installed images.
UnsignedPackage	Package does not have proper digital signature.
MemoryError	Memory error when installing package. Reboot may be necessary.
BadCertificate	Package does not have proper digital certificate.
DowngradeRevisionNotSupported	Using update to install some older versions is not supported.
PackageOpenError	Unable to open package. Make sure you have a correct IPS package.
CannotUpdateDVWhenTSEIsBusy	Unable to update Threat Suppression Engine packages while the system is busy reloading filters. Retry operation at a later time.

Device Maximum Values

Details the maximum values for X family devices.

The following table give the maximum values for configurable parameters of X family devices.

Table D–1: Device Maximum Values

Parameter	X5	X506
Firewall		
Rules	100	500
Security Zones	16	32
Services	125	200
Service Groups	25	50
Sessions	60,000	131,072
VPN		
Security Association	50	512
IKE Proposals	25	50
PPTP Sessions	128	1,000
L2TP Sessions	128	1,000
IPSec Tunnels not Default SA	50	512
IPSec Tunnels via Default SA	50	1,000

Table D–1: Device Maximum Values (Continued)

Parameter	X5	X506
Network		
IP Address Groups	25	200
Entries per IP Address Group	50	200
Virtual Interfaces	6	32
GRE Virtual Interfaces	4	100
Static Routes	100	500
RIP Routes	5,000	8,000
Schedules	25	100
Virtual Servers	25	100
DHCP Static Mapping	128	512
Certificates		
Local Certificates	5	25
Certificate Request	5	5
CA Certificate	5	25
Web Filter		
URL Patterns	200	1,000
Content Filter Default Cache Size	2 MB	4 MB
Users and Privileges		
Local Users	100	200
Privilege Groups	50	100

Glossary

action set

An integral part of an attack or peer-to-peer filter, action sets determine what the X family device does when a packet triggers a filter. An action set can contain more than one action, and can contain more than one type of action. The types of action that can be specified include the following:

- **Flow Control actions** — determines where a packet is sent after it is inspected. *Permit* allows a packet to reach its intended destination. *Block* discards a packet. A block action can also be configured to *quarantine* the host and/or perform a *TCP reset*. *Rate limit* enables you to define the maximum bandwidth available for the traffic stream.
- **Packet Trace action** — captures all or part of a suspicious packet for analysis depending on how the packet trace options are configured.

The system comes with a set of default action sets that are applied to groups of filters based on a category setting recommended by the Threat Management Center. For details, see [“category settings” on page 308](#). The default action sets can be customized for individual filters or groups of filters. You can also create new action sets. For additional details, see [“Action Sets” on page 44](#).

Adaptive Filter Configuration

This function allows you to configure IPS to protect against potential adverse affects of a defective filter. When Adaptive Configuration is turned on and the network is experiencing heavy loads, the X family device will automatically disable any filter that may be causing the congestion to prevent the device from entering High Availability mode and going offline. AFC settings are set to either Auto or Manual for the entire IPS. The default is Auto which means that AFC is on. AFC can also be turned on or off for specific filters.

aggregation period

The length of time during which multiple instances of a specific attack can occur before notification is sent to a contact.

Application Protection

Category of filter types that defend against known and unknown exploits that target applications and operating systems of workstations and servers on a network. These filters include a variety of attack protection and security policy filters. These filters detect specific recognition data to recognize an attempted attack and take specific courses of action that you define when an attempt is detected.

attack filter package

See [“Digital Vaccine Package” on page 309](#).

attack traffic

Packets traversing a network that match at least one Application Protection (see page 308) filter.

Category

Digital Vaccine filters are organized into three main Categories based on the type of protection provided: Application Protection (see page 308), Infrastructure Protection (see page 310), and Performance Protection (see page 311). These categories are used to organize and locate filters in the LSM web application.

category settings

Category settings are used to assign global configuration settings to filters within a category. For example, a *Vulnerability* filter responds to attack traffic based on the category settings for the *Application Protection* category while a *Network Equipment* filter would respond based on the category settings for the *Infrastructure Protection* category. Users can edit individual filters within a sub-category to override the category settings for the filter. Category settings consist of the following global parameters:

- **State** — determines whether filters within the sub-category are enabled or disabled. If a category is disabled, all filters in the Category are disabled.
- **Action Set** — determines the action set that filters within a Category will execute when a filter match occurs. If the *Recommended* action set is configured, filters within the category are configured with the settings recommended by the Digital Vaccine team. If required, you can override the category setting on individual filters by editing the filter to define custom settings.

Classless Inter-Domain Routing (CIDR)

An address format similar to an IP address except that it is followed by a slash (/) and a specified number of bits. The number of bits indicates the significant bits in the address. In the following example, the IP source address of a packet must match all 32 bits of the IP address specified:

10.3.4.5/32

Custom Shield Writer (CSW)

An optional, stand-alone, TippingPoint application to write custom filters that can be imported for use on devices.

Digital Vaccine Filters

Digital Vaccine Filters block attacks and other malicious traffic from the network. Filters come with a set of recommended (default) settings which specify the filter status (enabled or disabled), the type of action to be taken when the filter is triggered (action set defined to permit or block traffic and/or send a notification) and the Adaptive Filter Configuration (see page 60) setting (on or off). Users can accept the default settings, or override them based on network security needs. Digital Vaccine filters are categorized in the following groups: Application Protection (see page 308), Infrastructure Protection (see page 310), and Performance Protection (see page 311).

Digital Vaccine filters are created by the Threat Management team that monitors global network security threats and continually develops new attack filters which are automatically distributed to preemptively protect against the exploit of new and zero day vulnerabilities. Updates are distributed using Digital Vaccine Packages.

Digital Vaccine Package

Downloadable software update that includes Digital Vaccine filters that provide the most current IPS protection for your network. The Digital Vaccine Package is available from the [Threat Management Center \(TMC\)](https://tmc.tippingpoint.com) (<https://tmc.tippingpoint.com>). Devices can also be configured to download and install the Digital Vaccine packages automatically.

DDoS filters

Group of infrastructure protection filters that detect denial of service attacks which flood a network with requests, including traditional SYN floods, DNS request floods against nameservers, and attempts to use protected systems as reflectors or amplifiers in attacks against third parties. These filters detect direct flood attacks and attacks hidden within larger packets and requests. DDoS filters include the following filters: SYN Proxy, Connection Flood, and CPS Flood filters.

Exploit filters

Filters that protect software from malicious attacks across a network by detecting and blocking the request. Exploits are attacks against a network using weaknesses in software such as operating systems and applications. These attacks usually take the form of intrusion attempts and attempts to destroy or capture data. These filters are part of the Application Protection (see page 308) filter category.

filter

Policy consisting of rules and conditions used to detect and manage malicious traffic on a network. Each filter includes an [action set](#) with instructions for managing data when the filter is triggered and [category settings](#). The LSM includes various types of filters, including Digital Vaccine filters in the Performance Protection (see page 311), Application Protection (see page 308), Infrastructure Protection (see page 310) categories along with traffic management, traffic threshold, and DDoS filters.

Identity Theft filters

Filters protect end users from Phishing attacks by detecting and blocking connections to known Phish sites and attacks. A Phishing Attack is typically an email or web site which has been spoofed to appear as if it is from a well known financial or transaction institution. The attacks are usually geared to obtain account information from the end user. These filters are part of the Application Protection (see page 308) filter category.

IKE (Internet Key Exchange)

Internet Key Exchange (IKE) is used to negotiate the keying material that is used by the VPN encryption and integrity algorithms. IKE is a two-stage mechanism for automatically establishing IPSec tunnels with dynamically generated keying material. IKE uses UDP port number 500 and precedes the actual IPSec data flow.

IM filters

IM filters detect and control traffic from Instant Messaging applications such as Yahoo Messenger or MSN Messenger, chat, file transfer and photo sharing. These filters can be used to block the operation of the Instant Messaging application. Many of the IM filters can also be used to rate limit traffic from IM applications. These filters are part of the Performance Protection (see page 311) filter category.

Infrastructure Protection

Category of filter types that protect network bandwidth and network infrastructure elements such as routers and firewalls from attack using a combination of traffic normalization, DDoS protection, and application, protocol, and network equipment protection. These filters include DDoS, network equipment protection, and traffic normalization filters.

Intrusion Prevention System (IPS)

The TippingPoint Intrusion Prevention System in the X family device is an active network defense system that provides true intrusion prevention. Unlike intrusion detection systems, the IPS continually cleanses Internet and Intranet traffic, identifying and preventing attacks before damage to critical resources occurs, ensuring network integrity and ultimately improving return on investment.

IP filter

A filter that blocks traffic based on the source, destination, port, protocol, and other parameters of the traffic.

IP interface

An IP interface is the Layer 3 configuration, that is, the IP configuration for its set of security zones (and hence Ethernet ports within the security zone. IP interfaces provide the X family device with the IP interfaces that it needs for the network connections you require.

IPSec

A protocol used to create secure VPNs by encrypting and authenticating all IP packets. It uses the IKE protocol for key exchange and authentication. IPSec provides security at the network layer.

L2TP

Layer 2 Tunneling protocol, a protocol for tunnelling VPN (Virtual Private Network) traffic. L2TP is an extension to the Point-to-Point Tunneling Protocol (PPTP). L2TP supports multiple protocols and unregistered and privately administered IP addresses over the Internet. L2TP provides a more secure connection than the PPTP protocol.

Local Security Manager (LSM)

A browser-based management application that provides on-the-box administration, configuration, and reporting for a single X family device.

Network Equipment filters

Filters that detect and block the malicious attacks that target equipment accessible through a network. Network attacks can broadly or specifically seek access and data to corrupt on a network. These filters are part of the [Infrastructure Protection](#) filter category.

notification contacts

Recipients of alert messages. These contacts receive an email alert when a filter with the proper notification contacts settings triggers. Contacts include staff with email accounts and the SMS application.

P2P filters

Filters that use the same algorithms as attack filters, but which block peer-to-peer protocol traffic. These protocols are primarily used to share music and video files. They essentially turn a personal computer into a file server which make its resources as well as those of its host network available to the peer-to-peer community. These filters are part of the [Performance Protection](#) filter category.

packet trace

Allows you to capture all or part of a suspicious packet for analysis. You can set the packet trace priority and packet trace verbosity for action sets.

Performance Protection

Category of filter types that allow key applications to have prioritized access to bandwidth ensuring that mission critical applications have adequate performance during times of high congestion. These filters include misuse and abuse, IP, and congestion/mitigation filters.

Port Scan/Host Sweep filters

Filters that perform port scans and host sweeps to prevent any malicious code, attacks, and exceeded threshold limits for traffic. Each filter scans a specific type of port and protocol to block attacks against ports and hosts. These filters are part of the [Application Protection](#) filter category.

PPTP (Point-to-Point Tunneling Protocol)

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a virtual private network (VPN) across TCP/IP-based data networks. PPTP supports on-demand, multi-protocol, virtual private networking over public networks, such as the Internet.

rate limiting

Setting in an action set that defines a maximum bandwidth that can be used by traffic that matches filters assigned to that action set. Incoming traffic in excess of this bandwidth is dropped. If two or more filters use the same rate limiting action set, then all packets matching these filters share the bandwidth.

Reconnaissance filters

Reconnaissance filters monitor traffic for events that indicate network activity usually associated with common information gathering techniques used by attackers to launch more sophisticated attacks. These attacks search through your network using various methods to locate vulnerabilities. After the

attack has gathered data by probing your system and scanning your network, it continues with pointed attacks against those vulnerabilities. Reconnaissance filters look for these patterns and alert either the LSM or the SMS when an attack is detected. Port Scan/Host Sweep filters (see page 311) filters are included in this category. These filters are part of the [Application Protection](#) filter category.

RIP (Routing Information Protocol, RFC 2453)

RIP (Routing Information Protocol, RFC 2453) is a dynamic protocol that uses a distance vector algorithm to communicate route information with other routers in the network. RIP is well suited to small networks and uses a single metric *hop count* to determine distances. RIP periodically sends route advertisements every 30 seconds using UDP broadcast or multicast packets. The best route to a destination will be the one that passes through the fewest number of routers (lowest hop count) to reach its destination. A destination with a metric of 16 hops or more is considered to be unreachable or of infinite distance.

Security Management System (SMS)

A Linux management server and Java-based client application for managing multipleX family devices. It provides coordination across your system for administration, configuration, and monitoring, attack filter customization, centralized distribution of upgrades, and enterprise-wide reporting and trend analysis.

Security Profiles

A security profile is used to set up Digital Vaccine filters to monitor traffic passing on one or more virtual segments. The profile consists of category settings for the DV filters along with any user-defined filter overrides and IP address limits/exceptions. After a security profile is created, the device will begin monitoring traffic on the segments included in the profile using the specified the filter settings.

Security Policy

Security Policy refers to all of the mechanisms available on the device to protect and manage network traffic including traffic management profiles, security profiles (Digital Vaccine Filters), DDoS and Traffic Threshold filters. These profiles and filters are configured based on your network deployment and operational policy.

security zone

A security zone is a section of the network which is associated with a port or VLAN. Security zones enable you to logically segment your networks so that the X family device can apply policy rules and IPS filters to control the traffic passing between the zones.

SNMP Server

Provides access to interface counters and other statistics, configuration data, and general system information via the Simple Network Management Protocol (SNMP). The SNMP server must be enabled to use SMS management or to allow NMS access.

spyware filters

Spyware filters detect and block downloads, communications and popups sent via spyware.

Streaming Media filters

Streaming Media filters detect and control traffic from Streaming Media applications that deliver audio and video content utilizing IP protocols, typically UDP. Because these streaming media applications demand high bandwidth, the use of these applications can have a large negative impact on network performance. These filters can be used to block the operation of the Instant Messaging application. Many of the IM filters can also be used to rate limit traffic from IM applications. These filters are part of the Performance Protection (see page 311) filter category.

Traffic Normalization filters

Filters that block network traffic when the traffic is considered malicious. These filters allow you to set alerts to trigger when the system recognizes this traffic. Traffic pattern filters alert when network traffic varies from normal. These filters are part of the [Infrastructure Protection](#) filter category.

Threat Management Center (TMC)

A 3Com service center that monitors sensors around the world for the latest attack information and builds and distributes attack filters. The TMC is available at the following URL: <https://tmc.tippingpoint.com>

Threat Suppression Engine (TSE)

Blend of Application-Specific Integrated Circuits (ASICs) and network processors that detect threats and anomalies in your network traffic. The TSE scans and reacts to malicious attacks or anomalous traffic based on the configuration of the IPS security profiles, traffic management and traffic thresholds filters using the latest Digital Vaccine package updates.

Virus filters

Virus filters detect and block events triggered by viruses, worms, Trojans, backdoors, and other blended malware threats. These filters are part of the Application Protection (see page 308) filter category.

Vulnerabilities filters

Filters that detect any attempt to exploit a vulnerability in any application, operating system, or networked hardware device. These filters determine whether a vulnerability exists based on traffic requests and reaction by services. These filters are part of the Application Protection (see page 308) filter category.

Index

A

- access level, user 247
- action set 307
- action sets 44
 - Block 45
 - Block + Notify 45
 - Block + Notify + Trace 45
 - category 308
 - create 48
 - create, quarantine 51
 - Delete, Edit 48
 - flow control 44, 307
 - notification contacts 44
 - packet trace 44, 307
 - Permit + Notify 45
 - Permit + Notify + Trace 45
 - quarantine 48, 49
 - rate-limiting 49
 - Recommended 45
- adaptive filter
 - config 33, 37
 - events 60, 125
- administrator 247
- aggregation period 53, 307
- Application Protection
 - reconnaissance filters
 - filter tuning 36
 - port scans, host sweeps 35
 - settings 34
- authentication 246, 251
 - firewall 251
- Auto Refresh 11, 267
- automatic page refresh 267

B

- Block 45
- Block + Notify 45
- Block + Notify + Trace 45
- blocked streams 110
- boot time 14
- bridge mode 132, 150
 - enable 150
- browser certificates 271, 272, 273, 274, 277, 279

C

- category 308
 - action sets 44
- category settings, disable filter category, override 32
- certificate authority 274

- certificates 271
 - client authentication message 272
 - example 279
 - security alert 273
 - certificate authority 274
 - invalid certificate name 277
- Classless Inter-Domain Routing (CIDR) 308
- client authentication message 272
- clients, local 4
- configuration
 - segment 132
 - TSE 110, 112
- configure
 - NMS 235
 - remote system log 54, 106, 242
 - SMS 234
 - SNMP 234
 - TSE 59
- connection table timeout 58
- create
 - action sets 48
 - action sets, quarantine 51
 - notification contact 53
 - personal certificates 279
 - port configuration 55
 - traffic threshold filter 43
 - user 249
- critical thresholds 240
- Custom Shield Writer (CSW) 308
- customer support xiv

D

- DDoS 310
- delete
 - notification contact 54
 - port configuration 55
 - ports 56
 - Security Zone 136
- DHCP
 - add static reservation 175
 - Default external interface
 - configuration 142
- DHCP Server
 - lease duration, allow BOOTP clients 170
- DHCP status summary 13
- Digital Vaccine 222
 - update 222, 223
 - version 14
- disable filter category override 32
- disk usage default threshold 240
- DMZ, creating with a Virtual Server 64
- DNS
 - global settings, configuring 156
 - lookup 177
- download update signature 224

E

- edit port scan/host sweep filter 36
- email
 - failure 53
 - preferences 241
- events
 - adaptive filter 60, 125
 - blocked streams 110
 - rate limited streams 112
- exceptions
 - Application Protection 34
- expiration, password 266
- External Interface default configuration 142

F

- filters 309
 - action sets 44
 - adaptive filter config 33, 37
 - Application Protection
 - reconnaissance filters
 - filter tuning 36
 - port scans, host sweeps 35
 - settings 34
 - category 308
 - disable override 32
 - create traffic threshold 43
 - DDoS 310
 - exceptions
 - Application Protection 34
 - Infrastructure Protection traffic threshold filters 38
 - manage 23
 - notification contacts 52
 - rate-limiting 49
 - reset 35
 - update 222
- find network path 177
- firewall 63
 - adding an IP service 78
 - authentication 251
- full routed/NAT mode 132

G

- guide
 - audience xi
 - conventions xii
 - caution xiii
 - note xiv
 - tip xiv

- warning xiii
- related documentation xiv
- screen captures xiii

H

- health
 - Auto Refresh option 267
 - module 118
 - performance/throughput 120
 - system summary 12
- Health Monitor
 - default disk and memory thresholds 240
 - reset 240
- High Availability 217, 235
 - and bridge mode 150
 - configuration 237
 - failover 236
 - forcing state change 239
 - polling 237
 - standby operation 236
- host
 - quarantine 115
 - sweeps filters 35

I

- icons on launch bar 9, 10
- IGMP 163
- IKE (Internet Key Exchange) 310
- interface
 - launch bar 10
 - main pane 11
 - system summary 12
- Intrusion Prevention System (IPS) 310
- invalid certificate name 277
- IP address allocation for IP interfaces 142
- IP Address Groups
 - add an IP address to 155
 - create 155
 - delete IP address from 155
 - edit 155
- IP filter 310
- IPS 1
- IPSec 310
 - configuration 184
 - enable 188, 189

L

- launch bar 10
 - icons 10
 - icons on 9
- layout of LSM screen 8
- leases
 - status of 13
- leases, status of 13
- level, user access 247
- local clients 4
- Local Security Manager (LSM) 310
- Log pages
 - Auto Refresh option 267
- logging in 6

- logging mode 58
 - disable if network is congested 59
- logs
 - formats 1.4 292
 - reports
 - rate limit 123, 125
 - reset 99
 - system summary 13
- LSM
 - Auto Refresh 267
 - launch bar 10
 - login 6
 - main pane 11
 - overview 1
 - SMS configuration 4
 - system requirements 4
 - TippingPoint 1
 - packet statistics 13
 - screen layout 8
 - system summary 12

M

- main pane 11
- manage filters 23
- Managed Streams
 - Blocked Streams
 - find 111
 - flush 111
 - Quarantined Addresses
 - find 114
 - force quarantine 115
 - remove from quarantine 115
 - Rate-Limited Streams
 - find 113
 - flush 113
- management console 54
- memory usage 117
 - default threshold 240
- misuse and abuse 311
- model number 14
- module
 - health 118
 - Ethernet Ports 120
- multicast 163

N

- navigation
 - LSM 5
 - overview 8
- Network
 - DHCP status summary 13
- Network Congestion
 - modify the TSE global configuration 59
- Network DHCP status summary 13
- network tools
 - DNS lookup 177
 - find network path 177
 - packet capture 177
 - ping 178

- NMS 234
 - configure 235
- notification contacts 52, 311
 - create 53
 - delete 54
 - email failure 53
 - email preferences 241

O

- operator 247
- overview 1

P

- Packet Capture 177
- packet statistics 13
 - resetting 13
- password
 - expiration 266
 - security requirement for 268
- Peer-to-Peer filter 311
- performance 120
- Performance Wizard 120
- Permit + Notify 45
- Permit + Notify + Trace 45
- PIM-DM 163
- ping 178
- policy rules 63
- port 55
 - add 56
 - configuration 55
- port delete 56
- port scans filters 35
- product code 14
- product specification 14

Q

- quarantine
 - action set 48, 49
 - create action set 51
 - find quarantined hosts 114
 - force host into 115
 - remove hosts from 115
 - timeout 58

R

- rate limited streams 112
- rate-limiting 49, 311
- reboot 12, 13
- Recommended 45
- reconnaissance filters
 - filter tuning 36
 - port
 - scan/host sweep 35
- refresh screen 11
- related documentation xiv
- remote syslog format 301
- reports
 - rate limit 123, 125
 - top ten filters 122
- requirements, system 4

- reset
 - filters 35
 - packet statistics 13
 - TCP 45
- RIP, definition of 312
- role, user 247
- rollback
 - states, messages 303
- rules
 - firewall 63

S

- Schedules
 - Delete 81
 - Edit 81
- screen refresh 11
- Security Access Level
 - default setting, changing 268
 - username and password requirements 268
- security alert 273
 - certificate authority 274
 - invalid certificate name 277
- Security Management System 312
- security notes 5
- Security Zone 312
 - edit configuration, delete 136
- segment configuration 132
- signature, update
 - download 224
- SMS 312
 - configure 234
 - device under control of 233
 - NMS 235
- SNMP 234, 312
- software update 224
 - states, messages 303
- Static Reservation
 - add 175
 - for DHCP, delete 175
- super-user 247
- system requirements 4
- system status 12
- system summary
 - health 12
 - how to display 12
 - log summary 13
 - packet statistics 13
 - product specification 14
 - system status 12
 - versions 14
- System Summary page
 - Auto Refresh option 267

T

- TCP reset 45
- tech support xiv
- Threat Management Center xiv, 313
- Threat Suppression Engine
 - configuration
 - blocked streams 110
 - rate limited streams 112
- thresholds, critical 240
- throughput 120

- TippingPoint 1
- TMC xiv, 313
- Top Ten Filters reports 122
- TOS version 14
- traffic 121
- Traffic Threshold Filter 38
 - create, edit 43
- transparent DMZ - NAT/Routed LAN
 - mode 131
- transparent mode 131
- troubleshooting 281, 291
- TSE
 - blocked streams 110
 - Configure timeouts 59
 - port configuration 55
 - add 56
 - delete 56
 - rate limited streams 112

U

- update
 - Digital Vaccine
 - auto 222
 - manual 223
 - download signature 224
 - filter 222
 - software 224
 - states, messages 303
- user
 - access level 247
 - accounts
 - valid username and password, security access level 268
 - create 249
 - modify 249
 - username security requirements 268

V

- version information 219
 - system summary 14
- virtual interface 310
- Virtual Private Networks (see VPN)
- Virtual Server
 - Delete 83, 84
 - Edit 83, 84
- VPN
 - client access authentication 251
 - Configuration
 - IPSec SA Phase 2 negotiation 206
 - connections 182
 - definition of 313
 - Interoperability with other vendors
 - IPSec configuration 206
 - IPSec configuration 182

W

- web filtering, bypassing 251